

Rec'd PCT/PTO 22 OCT 2004  
PCT/JP 03/05322

日本国特許庁  
JAPAN PATENT OFFICE

25.04.03

別紙添付の書類に記載されている事項は下記の出願書類に記載されて  
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed  
with this Office

出願年月日

Date of Application:

2002年 4月25日

出願番号

Application Number:

特願2002-123502

[ST.10/C]:

[JP2002-123502]

REC'D 20 JUN 2003

WIPO PCT

出願人

Applicant(s):

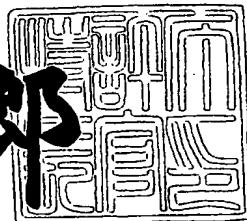
日本電気株式会社

PRIORITY DOCUMENT  
SUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH  
RULE 17.1(a) OR (b)

2003年 6月 2日

特許庁長官  
Commissioner,  
Japan Patent Office

太田信一郎



出証番号 出証特2003-3041465

【書類名】 特許願  
【整理番号】 33509933  
【あて先】 特許庁長官殿  
【国際特許分類】 H04Q 7/00  
                  H04B 7/26

## 【発明者】

【住所又は居所】 東京都港区芝五丁目7番1号 日本電気株式会社内  
【氏名】 百名 盛久

## 【特許出願人】

【識別番号】 000004237  
【氏名又は名称】 日本電気株式会社

## 【代理人】

【識別番号】 100093595

## 【弁理士】

【氏名又は名称】 松本 正夫

## 【手数料の表示】

【予納台帳番号】 057794  
【納付金額】 21,000円

## 【提出物件の目録】

【物件名】 明細書 1  
【物件名】 図面 1  
【物件名】 要約書 1  
【包括委任状番号】 9303563

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 移動通信網システム及び移動通信方式

【特許請求の範囲】

【請求項1】 移動通信網と、複数の外部網と、複数の移動端末と、複数のゲートウェイと、複数のアクセスポイントとから構成され、前記ゲートウェイが前記外部網と前記移動通信網とを接続し、前記アクセスポイントが前記移動端末を前記移動通信網に接続する構成の移動通信網システムにおいて、

前記移動通信網内の前記移動端末間でパケットを送受信する場合、前記外部網を介することなく、前記移動通信網上に用意された前記外部網毎に対応する仮想網を介して通信することを特徴とする移動通信網システム。

【請求項2】 移動通信網と、複数の外部網と、複数の移動端末と、複数のゲートウェイと、複数のアクセスポイントとから構成され、前記ゲートウェイが前記外部網と前記移動通信網とを接続し、前記アクセスポイントが前記移動端末を前記移動通信網に接続する構成の移動通信網システムにおいて、

前記移動通信網は前記外部網の各々に対応する仮想網を提供する手段を備え、  
前記ゲートウェイは前記外部網を対応する前記仮想網に接続する手段を備え、  
前記移動端末は任意の前記外部網用のセッションを前記アクセスポイントとの間に設定する手段を備え、

前記アクセスポイントは任意の前記セッションから受信したパケットを、当該セッションに対応する外部網用に用意された仮想網に転送する手段を備え、

前記アクセスポイントは任意の外部網に対応する前記仮想網から受信したパケットを、当該パケットのあて先である前記移動端末が前記外部網用に設定したセッションに転送する手段を備え、

前記移動端末と前記外部網との間に専用線接続を提供し、前記移動通信網内の前記移動端末間でパケットを送受信する場合、前記移動通信網上に用意された外部網用の仮想網を介して通信することを特徴とする移動通信網システム。

【請求項3】 前記移動端末が、現在接続されている現アクセスポイントから新たなアクセスポイントへハンドオーバーする場合、前記現アクセスポイントが、前記移動端末が設定した全ての前記セッションの情報を、前記新たなアクセ

ポイントへ転送する手段を備え、

移動端末がハンドオーバーする際に移動端末と外部網との専用線接続が途切れることなく継続できるように構成したことを特徴とする請求項2に記載の移動通信網システム。

**【請求項4】** 前記移動端末が、現在接続されている現アクセスポイントから新たなアクセスポイントへハンドオーバーする場合、前記新たなアクセスポイントは、前記現アクセスポイントから、前記移動端末が設定した全ての前記セッションの設定情報を取得する手段を備え、

移動端末がハンドオーバーする際に移動端末と外部網との専用線接続が途切れることなく継続できるように構成したことを特徴とする請求項2に記載の移動通信網システム。

**【請求項5】** 前記移動通信網内に移動管理ノードが配置され、

前記移動管理ノードは前記外部網毎に用意された複数の仮想移動管理ノードから構成され、

前記仮想移動管理ノードの各々が対応する前記外部網用に用意された前記仮想網との間でのみパケットの送受信を行う手段を備え、

前記移動端末は接続する前記外部網に対応する前記仮想移動管理ノードに位置情報を通知する手段を備え、

前記仮想移動管理ノードの各々は前記移動端末から通知された位置情報を保持する手段と、前記移動端末を先とするパケットを受信した場合、そのパケットを前記移動端末から通知された位置に転送する手段とを備え、

移動通信網上に前記外部網の各々に対応して用意された前記仮想網において、移動端末の位置を管理する構成としたことを特徴とする請求項2から請求項4の何れか一つに記載の移動通信網システム。

**【請求項6】** 前記移動通信網は制御・管理用仮想網を備え、

前記アクセスポイントや前記移動管理ノードを含む前記移動通信網内に配置されているノードが、互いの間でやり取りする制御用や管理用のパケットを前記制御管理用仮想網を介して送受信する手段と、前記制御管理用仮想網以外から受信した制御用や管理用のパケットを拒否する手段を備え、

前記移動通信網内に配置されているノード間通信の安全性を確保する構成としたことを特徴とする請求項2から請求項5の何れか一つに記載の移動通信網システム。

【請求項7】 移動通信網と、複数の外部網と、複数の移動端末と、複数のゲートウェイと、複数のアクセスポイントとから構成され、前記ゲートウェイが前記外部網と前記移動通信網とを接続し、前記アクセスポイントが前記移動端末を前記移動通信網に接続する構成の移動通信網の移動通信方式であって、

前記移動端末が任意の前記外部網用のセッションを前記アクセスポイントとの間に設定し、

前記アクセスポイントが任意の前記セッションから受信したパケットを、当該セッションに対応する前記外部網毎に用意された仮想網に転送し、

前記アクセスポイントが任意の外部網に対応する前記仮想網から受信したパケットを、当該パケットのあて先である前記移動端末が前記外部網用に設定したセッションに転送することにより、

前記移動端末と前記外部網との間に専用線接続を提供し、前記移動通信網内の前記移動端末間でパケットを送受信する場合、前記移動通信網上に用意された外部網用の仮想網を介して通信することを特徴とする移動通信方式。

【請求項8】 前記移動端末が、現在接続されている現アクセスポイントから新たなアクセスポイントへハンドオーバーする場合、前記現アクセスポイントが、前記移動端末が設定した全ての前記セッションの情報を、前記新たなアクセスポイントへ転送することを特徴とする請求項7に記載の移動通信方式。

【請求項9】 前記移動端末が、現在接続されている現アクセスポイントから新たなアクセスポイントへハンドオーバーする場合、前記新たなアクセスポイントが、前記現アクセスポイントから、前記移動端末が設定した全ての前記セッションの設定情報を取得することを特徴とする請求項7に記載の移動通信方式。

【請求項10】 前記移動通信網内に配置された移動管理ノードが、前記外部網毎に用意された複数の仮想移動管理ノードから構成され、

前記仮想移動管理ノードの各々が、対応する前記外部網用に用意された前記仮想網との間でのみパケットの送受信を行い、

前記移動端末が、接続する前記外部網に対応する前記仮想移動管理ノードに位置情報を通知し、

前記仮想移動管理ノードの各々が、前記移動端末から通知された位置情報を保持し、前記移動端末をあて先とするパケットを受信した場合、そのパケットを前記移動端末から通知された位置に転送することにより、

前記移動通信網上に前記外部網の各々に対応して用意された前記仮想網において、移動端末の位置を管理することを特徴とする請求項7から請求項9の何れか一つに記載の移動通信方式。

**【請求項11】** 前記移動通信網が、制御・管理用仮想網を備え、

前記アクセスポイントや前記移動管理ノード等の前記移動通信網内に配置されているノードが互いの間でやり取りする制御用や管理用のパケットを前記制御管理用仮想網を介して送受信し、前記制御管理用仮想網以外から受信した制御用や管理用のパケットを拒否することにより、

前記移動通信網内に配置されているノード間通信の安全性を確保することを特徴とする請求項7から請求項10の何れか一つに記載の移動通信方式。

#### 【発明の詳細な説明】

##### 【0001】

##### 【発明の属する技術分野】

本発明は、移動通信網システム及び移動通信方式に関し、特に、移動通信網が外部網と移動端末との間に専用線接続機能を提供する移動通信網システム及び移動通信方式に関する。

##### 【0002】

##### 【従来の技術】

動通信網が外部網と移動端末との間に専用線接続機能を提供する従来技術としては、ETSI (European Telecommunications Standards Institute) や3GPP (Third Generation Partnership Project) において規定された移動通信技術であるGPRS (GENERAL PACKET RADIO SERVICE) がある。GPRSは端末の移動をサポートするとともに、移動端

末を特定の外部網に接続する専用線接続機能を提供する。

#### 【0003】

また、IETF (Internet Engineering Task Force: インターネット・エンジニアリング・タスク・フォース)において開発された移動制御技術としてMobile IP (モバイル・アイピー) (RFC 2002) が、プライベート網技術としてIPSEC (アイ・ピー・セック) 等がある。これらの技術を組み合わせることにより、端末の移動をサポートし、移動端末と外部網との間に専用線接続を実現できる。

#### 【0004】

また、移動端末を外部網に接続するため移動通信網のコア網に仮想プライベート網技術を使用するという技術提案があり、その一例としては、例えば、  
<http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/itsolutions/network/deploy/depovg/ieee802.asp>  
 に公開されているものがある。

#### 【0005】

##### 【発明が解決しようとする課題】

上述した従来の技術においては、以下に述べるような種々の問題点があった。

#### 【0006】

上述した従来のGPRSでは、外部網とのゲートウェイと移動端末との間にトンネルを設定し、全ての通信はこのトンネルを介して行う。移動端末間で通信を行う場合、移動端末が送信したパケットはトンネルを介して外部網とのゲートウェイに送信され、再び外部網とのゲートウェイからトンネルを介して通信相手の移動端末に折り返し送信される。

#### 【0007】

このためパケットの遅延が大きく、また移動通信網内の帯域を浪費するため回線の使用効率が悪いという問題があった。

#### 【0008】

また、複数の移動端末へのマルチキャスト通信の場合も、外部網とのゲートウェイにおいて移動端末のトンネル毎にマルチキャストパケットがコピーされて送

信されるため、網内の帯域を浪費し、回線の使用効率が悪いという問題があった

## 【0009】

一方、Mobile IPとIPSECを使用したIPベースの移動通信網の場合、移動網と外部網はIP網であることが前提である。このフラットなIP網上でまず、Mobile IPにより端末の移動がサポートされる。そして、さらに専用線接続機能を提供するために、移動通信網と外部網との間にはゲートウェイが配置され、移動端末とゲートウェイの間にIPSECによりトンネルが設定される。

## 【0010】

このように、Mobile IPとIPSECを使用したIPベースの移動通信網において専用線接続機能を提供する場合、全てのパケットがトンネルを介してやり取りされるため、この構成ではGPRSの場合と同様の問題が生じる。

## 【0011】

なお、別の構成として、移動端末間で通信を行う場合は、移動端末間にIPSecのトンネルを直接設定し、ゲートウェイを介した折り返し通信を行なわずに済むようにすることも可能である。ただし、この構成ではマルチキャスト通信の場合の問題は解決できない。また、通信相手の移動端末が多い場合、トンネルの管理の手間が多いという問題がある。

## 【0012】

また、Mobile IPやIPSECを使用したIPベースの移動通信網の場合、移動通信網内のノードに外部から自由にアクセス可能であるためセキュリティ機能が必要である。例えば、アクセスポイント間でハンドオーバーを行う場合はアクセスポイント間のハンドオーバー要求やハンドオーバー通知のパケットはアクセスポイント間に認証用のセキュリティアソシエーションを行なう必要があり、このためにはアクセスポイント間に認証用のセキュリティアソシエーションをあらかじめ確立しておく必要がある。このような手法はアクセスポイントの数が増えてくると、セキュリティアソシエーションの管理が煩雑になるという問題がある。

## 【0013】

また、移動通信網のコア網に仮想プライベート網技術を使用し、外部網への接続を提供する場合、従来技術では端末の移動時にプライベート網接続が途切れるという問題がある。

## 【0014】

本発明は上記の事情を考慮してなされたものであり、その第1の目的は、移動端末で通信を行う場合の回線使用効率の改善を実現する移動通信網システム及び移動通信方式を提供することにある。

## 【0015】

本発明の他の目的は、移動端末のマルチキャストの通信において、回線使用効率の改善を実現する移動通信網システム及び移動通信方式を提供することにある。

## 【0016】

また、本発明の他の目的は、移動端末間またはノード間でセキュリティーアソシエーションを確立する手間が不要となる移動通信網システム及び移動通信方式を提供することにある。

## 【0017】

また、本発明の他の目的は、移動端末がハンドオーバーする際に移動端末と外部網との専用線接続が途切れることなく継続できる移動通信網システム及び移動通信方式を提供することにある。

## 【0018】

## 【課題を解決するための手段】

上記目的を達成する本発明は、移動通信網と、複数の外部網と、複数の移動端末と、複数のゲートウェイと、複数のアクセスポイントとから構成され、前記ゲートウェイが前記外部網と前記移動通信網とを接続し、前記アクセスポイントが前記移動端末を前記移動通信網に接続する構成の移動通信網システムにおいて、前記移動通信網内の前記移動端末間でパケットを送受信する場合、前記外部網を介すことなく、前記移動通信網上に用意された前記外部網毎に対応する仮想網を介して通信することを特徴とする。

## 【0019】

請求項2の本発明は、移動通信網と、複数の外部網と、複数の移動端末と、複数のゲートウェイと、複数のアクセスポイントとから構成され、前記ゲートウェイが前記外部網と前記移動通信網とを接続し、前記アクセスポイントが前記移動端末を前記移動通信網に接続する構成の移動通信網システムにおいて、前記移動通信網は前記外部網の各々に対応する仮想網を提供する手段を備え、前記ゲートウェイは前記外部網を対応する前記仮想網に接続する手段を備え、前記移動端末は任意の前記外部網用のセッションを前記アクセスポイントとの間に設定する手段を備え、前記アクセスポイントは任意の前記セッションから受信したパケットを、当該セッションに対応する外部網用に用意された仮想網に転送する手段を備え、前記アクセスポイントは任意の外部網に対応する前記仮想網から受信したパケットを、当該パケットのあて先である前記移動端末が前記外部網用に設定したセッションに転送する手段を備え、前記移動端末と前記外部網との間に専用線接続を提供し、前記移動通信網内の前記移動端末間でパケットを送受信する場合、前記移動通信網上に用意された外部網用の仮想網を介して通信することを特徴とする。

## 【0020】

請求項3の本発明の移動通信網システムは、前記移動端末が、現在接続されている現アクセスポイントから新たなアクセスポイントへハンドオーバーする場合、前記現アクセスポイントが、前記移動端末が設定した全ての前記セッションの情報を、前記新たなアクセスポイントへ転送する手段を備え、移動端末がハンドオーバーする際に移動端末と外部網との専用線接続が途切れることなく継続できるように構成したことを特徴とする。

## 【0021】

請求項4の本発明の移動通信網システムは、前記移動端末が、現在接続されている現アクセスポイントから新たなアクセスポイントへハンドオーバーする場合、前記新たなアクセスポイントは、前記現アクセスポイントから、前記移動端末が設定した全ての前記セッションの設定情報を取得する手段を備え、移動端末がハンドオーバーする際に移動端末と外部網との専用線接続が途切れることなく継続できるように構成したことを特徴とする。

## 【0022】

請求項5の本発明の移動通信網システムは、前記移動通信網内に移動管理ノードが配置され、前記移動管理ノードは前記外部網毎に用意された複数の仮想移動管理ノードから構成され、前記仮想移動管理ノードの各々が対応する前記外部網用に用意された前記仮想網との間でのみパケットの送受信を行う手段を備え、前記移動端末は接続する前記外部網に対応する前記仮想移動管理ノードに位置情報を通知する手段を備え、前記仮想移動管理ノードの各々は前記移動端末から通知された位置情報を保持する手段と、前記移動端末をあて先とするパケットを受信した場合、そのパケットを前記移動端末から通知された位置に転送する手段とを備え、移動通信網上に前記外部網の各々に対応して用意された前記仮想網において、移動端末の位置を管理する構成としたことを特徴とする。

## 【0023】

請求項6の本発明の移動通信網システムは、前記移動通信網は制御・管理用仮想網を備え、前記アクセスポイントや前記移動管理ノードを含む前記移動通信網内に配置されているノードが、互いの間でやり取りする制御用や管理用のパケットを前記制御管理用仮想網を介して送受信する手段と、前記制御管理用仮想網以外から受信した制御用や管理用のパケットを拒否する手段を備え、前記移動通信網内に配置されているノード間通信の安全性を確保する構成としたことを特徴とする。

## 【0024】

請求項7の本発明は、移動通信網と、複数の外部網と、複数の移動端末と、複数のゲートウェイと、複数のアクセスポイントとから構成され、前記ゲートウェイが前記外部網と前記移動通信網とを接続し、前記アクセスポイントが前記移動端末を前記移動通信網に接続する構成の移動通信網の移動通信方式であって、前記移動端末が任意の前記外部網用のセッションを前記アクセスポイントとの間に設定し、前記アクセスポイントが任意の前記セッションから受信したパケットを、当該セッションに対応する前記外部網毎に用意された仮想網に転送し、前記アクセスポイントが任意の外部網に対応する前記仮想網から受信したパケットを、当該パケットのあて先である前記移動端末が前記外部網用に設定したセッション

に転送することにより、前記移動端末と前記外部網との間に専用線接続を提供し、前記移動通信網内の前記移動端末間でパケットを送受信する場合、前記移動通信網上に用意された外部網用の仮想網を介して通信することを特徴とする。

## 【0025】

請求項8の本発明の移動通信方式は、前記移動端末が、現在接続されている現アクセスポイントから新たなアクセスポイントへハンドオーバーする場合、前記現アクセスポイントが、前記移動端末が設定した全ての前記セッションの情報を、前記新たなアクセスポイントへ転送することを特徴とする。

## 【0026】

請求項9の本発明の移動通信方式は、前記移動端末が、現在接続されている現アクセスポイントから新たなアクセスポイントへハンドオーバーする場合、前記新たなアクセスポイントが、前記現アクセスポイントから、前記移動端末が設定した全ての前記セッションの設定情報を取得することを特徴とする。

## 【0027】

請求項10の本発明の移動通信方式は、前記移動通信網内に配置された移動管理ノードが、前記外部網毎に用意された複数の仮想移動管理ノードから構成され、前記仮想移動管理ノードの各々が、対応する前記外部網用に用意された前記仮想網との間でのみパケットの送受信を行い、前記移動端末が、接続する前記外部網に対応する前記仮想移動管理ノードに位置情報を通知し、前記仮想移動管理ノードの各々が、前記移動端末から通知された位置情報を保持し、前記移動端末をあて先とするパケットを受信した場合、そのパケットを前記移動端末から通知された位置に転送することにより、前記移動通信網上に前記外部網の各々に対応して用意された前記仮想網において、移動端末の位置を管理することを特徴とする。

## 【0028】

請求項11の本発明の移動通信方式は、前記移動通信網が、制御・管理用仮想網を備え、前記アクセスポイントや前記移動管理ノード等の前記移動通信網内に配置されているノードが互いの間でやり取りする制御用や管理用のパケットを前記制御管理用仮想網を介して送受信し、前記制御管理用仮想網以外から受信した

制御用や管理用のパケットを拒否することにより、前記移動通信網内に配置されているノード間通信の安全性を確保することを特徴とする。

## 【0029】

以上の構成と手段により、移動端末と外部網との間でパケット送受信が可能となり、さらに、同じ外部網に接続される移動端末同士で通信を行う場合、移動端末からその外部網用のセッションを介して送信されたパケットはアクセスポイントを出た後は、その外部網用の仮想網を経由して、通信相手の移動端末が接続されているアクセスポイントへ直接転送される。そして、通信相手の移動端末がその外部網用に設定したセッションを介して通信相手の移動端末へ届けられる。また、マルチキャストパケットはその外部網用の仮想網の上を通常のマルチキャストパケットとして送信され、アクセスポイントに到達した後、その外部網用のセッションを介して移動端末に届けられることとなる。

## 【0030】

## 【発明の実施の形態】

以下、本発明の好ましい実施の形態について図面を参照して詳細に説明する。

## 【0031】

## (第1の実施の形態)

図1を用いて本発明の第1の実施の形態について説明する。図1は網全体の構成を示す。網全体は、複数の外部網EX1、EX2、EX3とこれに接続される移動通信網MNW、そして移動通信網MNWを介して1つ以上の外部網に接続される複数の移動端末X、Y、Zから構成される。なお、外部網の数や移動端末の数は特定の数に限定されない。

## 【003.2】

移動通信網MNWは、コア網CNと、複数のアクセス網ANa、ANb、ANcと、複数の無線ドロップ回線と、複数の有線ドロップ回線、コア網CNと外部網を接続する外部網ゲートウェイEGW1、EGW2、EGW3と、コア網CNとアクセス網を接続するアクセス網ゲートウェイAGWa、AGWb、AGWcと、アクセス網と無線ドロップ回線とを接続する無線アクセスポイントAPa1と、APa2、APb1、APb2と、アクセス網と有線ドロップ回線とを接続す

る有線アクセスポイントAPc1、APc2とから構成される。なお、アクセス網の数、アクセスポイントの数は特定の数に限定されない。

#### 【0033】

図2はコア網CNの論理的な構成を示す。コア網CNは、マルチプロトコルラベルスイッチングなどの既存の仮想プライベート網技術を使用しており、物理的なコア網CN上に複数の仮想コア網が多重されている。この例では外部網(1)用仮想コア網VCN1、外部網(2)用仮想コア網VCN2、外部網(3)用仮想コア網VCN3、制御管理用仮想コア網VCNSが多重されている。

#### 【0034】

図3はアクセス網の論理的な構成を示す。アクセス網は、マルチプロトコルラベルスイッチングなどの既存の仮想プライベート網技術を使用しており、物理的なアクセス網ANA上に、複数の仮想アクセス網が多重されている。この例では外部網(1)用仮想アクセス網VANA1、外部網(2)用仮想アクセス網VANA2、外部網(3)用仮想アクセス網VANA3、制御管理用仮想アクセス網VANASが多重されている。

#### 【0035】

図4は無線ドロップ回線または有線ドロップ回線の論理的な構成を示す。物理的なドロップ回線LD上には、通信用チャネルCH1と認証用チャネルCH2との間のセッションが多重される。通信用チャネルCH1上には、各移動端末と各外部網との間のセッションが多重される。ここでは、移動端末(x)Xと外部網(1)EX1との間のセッションSx1、移動端末(x)Xと外部網(2)EX2との間のセッションSx2、移動端末(y)Yと外部網(1)EX1との間のセッションSy1が通信用チャネルCH1上に多重されている。

#### 【0036】

認証用チャンネルCH2と通信用チャンネルCH1の識別と多重分離に関しては、ドロップ回線LDのリンク技術がこのための専用の仕組みを用意していれば、それを利用する。また、リンク技術がそのような仕組みを用意していない場合、コネクション指向型のリンク技術の場合は、コネクション識別子を利用して認証用チャネルCH2と通信用チャネルCH1を多重し、コネクションレス型のリンク

ク技術の場合は、パケットタイプ識別子等を利用して認証用チャネルCH2と通信用チャネルCH1を多重する。

#### 【0037】

また、移動端末と外部網との間のセッションの識別と多重分離に関しては、リンク技術がこのための専用の仕組みを用意していればそれを利用する。また、リンク技術がそのような仕組みを用意していない場合、コネクション指向型のリンク技術の場合は、コネクション識別子を利用してセッションを多重分離し、コネクションレス型のリンク技術の場合は、パケットタイプ識別子や仮想ネットワーク識別子等を利用してセッションを多重分離する。

#### 【0038】

図5は外部網ゲートウェイの構成を示す。外部網ゲートウェイEGW1は、外部網側送受信機TR01、外部網ゲートウェイ機能EGF、外部網ゲートウェイ管理機能EGCF、仮想コア網多重分離機能CMUX1、コア網側送受信機TR02から構成される。

#### 【0039】

外部網側送受信機TR01は、外部網EX1と接続され、パケットの送受信を行う。

#### 【0040】

コア網側送受信機TR02は、コア網CNと接続され、パケットの送受信を行う。

#### 【0041】

仮想コア網多重分離機能CMUX1は、コア網側送受信機TR02から入力されたパケットを仮想コア網毎に分離し、接続されている外部網EX1に対応する外部網（1）用仮想コア網VCN1上を転送されてきたパケットを外部網ゲートウェイEGFに入力し、また、制御管理用仮想コア網VCNSを転送されてきたパケットを外部網ゲートウェイ管理機能EGCFに入力する。

#### 【0042】

また、仮想コア網多重分離機能CMUX1は、外部網ゲートウェイEGFから入力された対応する外部網（1）用仮想コア網VCN1に転送し、外部網ゲート

ウェイ管理機能E G C F から入力されたパケットを制御管理用仮想コア網V C N S に転送し、これらの仮想コア網を多重してコア網側送受信機T R 0 2 に出力する。

## 【0043】

外部網ゲートウェイ機能E G F は、外部網E X 1 とコア網C Nとの間のパケットのルーティングやフィルタリングを行う。

## 【0044】

外部網ゲートウェイ管理機能E G C F は、外部網ゲートウェイ機能E G Fへの経路設定やフィルタリングの設定を行う。

## 【0045】

図6にアクセス網ゲートウェイの構成を示す。アクセス網ゲートウェイA N G a は、コア網側送受信機T R 0 3 a 、仮想コア網多重分離機能C M U X a 、外部網（1）用仮想アクセス網ゲートウェイV A G W 1 a 、外部網（2）用仮想アクセス網ゲートウェイV A G W 2 a 、外部網（3）用仮想アクセス網ゲートウェイV A G W 3 a 、制御管理用仮想アクセス網ゲートウェイV A G W S a 、仮想アクセス網多重分離機能A M U X 1 a 、アクセス網側送受信機T R 0 4 a 、から構成される。

## 【0046】

コア網側送受信機T R 0 3 a は、コア網C Nと接続され、パケットの送受信を行う。

## 【0047】

アクセス網側送受信機T R 0 4 a は、アクセス網A N a と接続され、パケットの送受信を行う。

## 【0048】

仮想コア網多重分離機能C M U X a は、コア網側送受信機T R 0 3 a から入力されたパケットを仮想コア網毎に分離し、外部網（1）用仮想コア網V C N 1 から受信したパケットは外部網（1）用仮想アクセス網ゲートウェイV A G W 1 a に出力し、外部網（2）用仮想コア網V C N 2 、外部網（3）用仮想コア網V C N 3 、管理制御用仮想コア網V C N S についても同様の処理を行う。

## 【0049】

また、仮想コア網多重分離機能CMUX1aは、外部網（1）用仮想アクセス網ゲートウェイVAGW1aから入力されたパケットを外部網（1）用仮想コア網上VCN1に出力し、外部網（2）用仮想アクセス網ゲートウェイVAGW2a、外部網（3）用仮想アクセス網ゲートウェイVAGW3a、制御管理用仮想アクセス網ゲートウェイVAGWSaについても同様の処理を行い、各仮想コア網を多重して、コア網側送受信機TR03aに出力する。

## 【0050】

仮想アクセス網多重分離機能AMUX1aは、アクセス網側送受信機TR04aから入力されたパケットを仮想アクセス網毎に分離し、外部網（1）用仮想アクセス網VANa1から受信したパケットは外部網（1）用仮想アクセス網ゲートウェイVAGW1aに出力し、外部網（2）用仮想アクセス網VANa2、外部網（3）用仮想アクセス網VANa3、管理制御用仮想アクセス網VANaSについても同様の処理を行う。

## 【0051】

また、仮想アクセス網多重分離機能AMUX1aは、外部網（1）用仮想アクセス網ゲートウェイVAGW1aから入力されたパケットを外部網（1）用仮想アクセス網上VANa1に出力し、外部網（2）用仮想アクセス網ゲートウェイVAGW2a、外部網（3）用仮想アクセス網ゲートウェイVAGW3a、制御管理用仮想アクセス網ゲートウェイVAGWSaについても同様の処理を行い、各仮想アクセス網を多重して、アクセス網側送受信機TR04aに出力する。

## 【0052】

外部網（1）用仮想アクセス網ゲートウェイ機能VAGW1aは、外部網（1）用仮想コア網VCN1と外部網（1）用仮想アクセス網VANa1との間のパケットのルーティングやフィルタリングを行う。外部網（2）用仮想アクセス網ゲートウェイ機能VAGW2a、外部網（3）用仮想アクセス網ゲートウェイ機能VAGW3aについても同様である。

## 【0053】

制御管理用仮想アクセス網ゲートウェイ機能VAGWSaは、上述した機能に

加えて、各仮想アクセス網ゲートウェイ機能VAGWa1、VAGWa2、VAGWa3への経路設定やフィルタリングの設定を行う。

## 【0054】

図7に移動端末の構成を示す。移動端末Xは、無線送受信機TR05、チャネル多重分離機能CHMUX1、パケット認証機能PAUTH1、セッション多重分離機能SMUX、端末認証機能TAUTH2、複数のホーム網との通信エンティティENT1、ENT2から構成される。

## 【0055】

無線送受信機TR05は、無線ドロップ回線との間でパケットの送受信を行う

## 【0056】

チャネル多重分離機能CHMUX1は、無線ドロップ回線上の認証用チャネルCCHと通信用チャネルTCHの多重分離を行う。認証用チャネルCCH上のパケットは、端末認証機能TAUTH2との間で送受され、通信用チャネルTCH上のパケットはパケット認証機能PAUTH1との間で送受される。

## 【0057】

端末認証機能TAUTH2は、図8に示す移動通信網情報管理テーブルと図9に示すホーム網情報管理テーブル、図10に示すセッション情報管理テーブルを有する。

## 【0058】

移動通信網情報管理テーブル（図8）は、端末ID110と移動通信網－移動端末間セキュリティアソシエーション111を持つ。端末ID110は、移動通信網内で端末を一意に識別するIDである。移動通信網－移動端末間セキュリティアソシエーション111とは、移動通信網と移動端末間との間で相互に認証を行うための情報である。これらの情報はあらかじめ移動端末Xに設定されているものとする。

## 【0059】

ホーム網情報管理テーブル（図9）は、ホーム網ID210とホーム網用端末ID220とホーム網－移動端末間セキュリティアソシエーション230の組が

らなる情報を1つ以上持つ。ホーム網ID210は、ホーム網を一意に識別するIDである。端末ID220は、ホーム網内で端末を一意に識別するIDである。ホーム網-移動端末間セキュリティアソシエーション230とは、ホーム網と移動端末間との間で認証を行うための情報である。これらの情報はあらかじめ移動端末Xに設定されているものとする。

## 【0060】

セッション情報管理テーブル（図10）は、ホーム網ID310とアクセスポイントID320とアクセスポイント-移動端末間セキュリティアソシエーション330とセッションID340とリンク情報350の組からなる情報を1つ以上持つ。

## 【0061】

これらの情報は、移動端末Xが後述の端末認証を行ったときに設定される。アクセスポイントID320は、端末が現在接続されているアクセスポイントのIDである。アクセスポイント-移動端末間セキュリティアソシエーション330とは、アクセスポイントと端末間で送受されるパケットのうち認証要求や認証応答以外のパケットを認証するための情報である。セッションID340は、アクセスポイントの間に設定されたセッションを識別するIDであり、セッションはホーム網との通信毎に用意される。リンク情報350とは、このセッションの識別や多重分離のために使用するリンク固有の情報である。リンク情報350は、使用するリンク技術に依存し、コネクション識別子、仮想プライベート網識別子などである。

## 【0062】

パケット認証機能PAUTH1は、チャネル多重分離機能CHMUX1から入力されたパケットを、前述のアクセスポイント-移動端末間セキュリティアソシエーション330に基づき認証し、認証されたパケットのみをセッション多重分離機能SMUXへ出力する。

## 【0063】

また、パケット認証機能PAUTH1は、セッション多重分離機能SMUXから入力されたパケットに前述のアクセスポイント-移動端末間セキュリティアソ

シェーション330に基づき認証コードを付加して、チャネル多重分離機能CH MUX1に入力する。

【0064】

セッション多重分離機SMUXは、前述のリンク情報350に基づき、パケット認証機能PAUTH1から入力されたパケットがどのセッションに属するかを判定し、対応するホーム網の通信エンティティENT1またはENT2へ渡す。また、セッション多重分離機能SMUXは、ホーム網の通信エンティティENT1及びENT2から渡されたパケットを対応するセッションのリンク情報350を用いて送信するように設定し、パケット認証機能PAUTH1へ出力する。

【0065】

図13を用いて端末認証の手順を説明する。

【0066】

端末認証機能TAUTH2は、移動端末Xがホーム網と通信を開始するときに、図11に示す認証要求パケット400を生成し、アクセスポイントに送信する。認証要求パケットの生成に際して、移動端末Xが最初に移動通信網に接続する場合、移動端末は旧アクセスポイントID401には何も設定しない。また、以前接続されていたアクセスポイントがある場合、移動端末は旧アクセスポイントID401にそのアクセスポイントのID320を設定する（ステップS131）。

【0067】

また、認証要求パケットの移動端末ID402、ホーム網ID404、ホーム網用移動端末ID405には移動通信網情報管理テーブル（図8）、ホーム網情報管理テーブル（図9）に基づき適切な情報が設定される。さらに、移動通信網用移動端末認証コード403には移動通信網-移動端末間セキュリティアソシエーション101に基づき、移動通信網が移動端末を認証するために必要な情報が設定され、ホーム網用移動端末認証コード406にはホーム網-移動端末間セキュリティアソシエーション230に基づき、ホーム網が移動端末Xを認証するために必要な情報が設定される。上記のように値を設定して認証要求パケット400を生成し（ステップ132）、アクセスポイントに送信する（ステップ133）。

)。

## 【0068】

これに対して、アクセスポイントは図12に示す認証応答パケットを返信する。返信された認証応答パケットを受信し（ステップ134）、認証応答パケットに設定されている認証結果502が成功であれば、認証応答パケットに設定されているアクセスポイントID501、アクセスポイント-移動端末間セキュリティアソシエーションの情報506とセッションID507、リンク情報508はセッション情報管理テーブルに保存される（ステップ135）。

## 【0069】

図14は無線アクセスポイントの構成である。無線アクセスポイントAPa1は、アクセス網側送受信機TR06a、仮想アクセス網多重分離機能AMUX2a、セッション-外部網マッピング機能MAP1、アクセスポイント制御管理機能APM1、端末認証機能TAUTH1、パケット認証機能PAUTH2、セッション情報ハンドオーバー機能HOF1、セッション情報管理テーブルSMT1、チャネル多重分離機能CHMUX2、無線送受信機TR07aから構成される。

## 【0070】

アクセス網側送受信機TR06aは、アクセス網ANaと接続され、パケットの送受信を行う。

## 【0071】

無線送受信機TR07aは、無線ドロップ回線との間でパケットの送受信を行う。

## 【0072】

仮想アクセス網多重分離機能AMUX2aは、アクセス網側送受信機TR06aから入力されたパケットを仮想アクセス網毎に分離し、外部網（1）用仮想アクセス網VANA1、外部網（2）用仮想アクセス網VANA2、外部網（3）用仮想アクセス網VANA3上のパケットをセッション-外部網マッピング機能MAP1に入力し、管理制御用仮想コア網VANAS上のパケットをアクセスポイント制御管理機能APM1に入力する。

## 【0073】

また、仮想アクセス網多重分離機能AMUX2aは、セッションー外部網マッピング機能MAP1から入力された外部網（1）用仮想アクセス網VANa1、外部網（2）用仮想アクセス網VANa2、外部網（3）用仮想アクセス網VANa3向けのパケットと、アクセスポイント制御管理機能APM1から入力された制御管理用仮想アクセス網VANaS向けのパケットを、各仮想アクセス網上に多重して、アクセス網側送受信機TR06aに出力する。

## 【0074】

チャネル多重分離機能CHMUX2は、無線送受信機TR07aから入力された信号をチャネル毎に分離し、通信用チャネルをパケット認証機能PAUTH2に入力し、認証用チャネルを端末認証機能TAUTH1に入力する。また、パケット認証機能PAUTH1から入力されたパケットを通信用チャネル上に多重し、端末認証機能TAUTH1から入力されたパケットを認証用チャネル上に多重して無線送受信機TR07aへ出力する。

## 【0075】

セッション情報管理テーブルSMT1は、図15に示す内容を保持する。移動端末ID(610)とその端末が接続している外部網ID(620)、移動端末からのパケットを認証するためのアクセスポイントー移動端末間セキュリティアソシエーション(630)、移動端末と外部網との間のセッションを識別するセッションID(640)、セッションを識別するためのリンク情報(650)であり、意味は移動端末に設定されたものと同じである。これらの情報は移動端末が最初に網に接続し、端末認証を行ったときに、端末認証機能により後述の手順に基づき設定される。

## 【0076】

パケット認証機能PAUTH2は、チャネル多重分離機能CHMUX2から入力されたパケットをセッション情報管理テーブル（図15）に保持されているアクセスポイントー移動端末間認証用セキュリティアソシエーション630に基づき認証し、セッションー外部網マッピング機能MAP1へ出力する。

## 【0077】

また、パケット認証機能P A U T H 2は、セッションー外部網マッピング機能MAP 1から入力されたパケットに対して、セッション情報管理テーブル（図15）に保持されているアクセスポイントー移動端末間認証用セキュリティアソシエーション630に基づき認証用コードを付加した上でチャネル多重分離機能C H M U X 2に出力する。

## 【0078】

セッションー外部網マッピング機能MAP 1は、パケット認証機能P A U T H 2から入力されたパケットをチェックし、セッション情報管理テーブル（図15）に保持されているリンク情報650に基づきセッションを識別する。そして、このセッション対応する外部網I D 620に基づき、適切な外部網用の仮想アクセス網に振り分け、仮想アクセス網多重分離機能A M U X 2 aに入力する。

## 【0079】

また、セッションー外部網マッピング機能MAP 1は、仮想アクセス網多重分離機能A M U X 2 aから入力されたパケットをチェックし、セッション情報管理テーブル（図15）に保持されている外部網I D 620と移動端末I D 610に基づきセッションを識別する。そして、このセッションに対応する適切なリンク情報を使用して送信するように設定し、パケット認証機能P A U T H 2へ出力する。

## 【0080】

なお、移動端末から受信したパケットのあて先の移動端末が同じアクセスポイント配下にいる場合は、セッションー外部網マッピング機能MAP 1はパケットをそのまま折り返して送信する。

## 【0081】

アクセスポイント制御管理機能A P M 1は、端末認証機能T A U T H 1とセッション情報ハンドオーバー機能H O F 1から入力されたパケットを仮想アクセス網多重分離機能A M U X 2 aに出力し、仮想アクセス網多重分離機能A M U X 2 aから入力されたパケットを分離して、端末認証機能T A U T H 1とセッション情報ハンドオーバー機能H O F 1に出力する。

## 【0082】

図2.0に示すフローチャートを用いて、端末認証の手順を説明する。

[0083]

端末認証機能T A U T H 1は、移動端末から受信した図1 1に示す認証要求パケットをチャネル多重分離機能C H M U X 2から入力されると、図1 6に示す認証要求パケットを生成し、移動網認証サーバに送信するためにアクセスポイント制御管理機能A P M 1に出力する。

[0084]

また、端末認証機能TAUH1は、移動通信網認証サーバから受信した図17に示す認証応答パケットをアクセスポイント制御管理機能APM1から入力されると、認証応答パケットの認証結果(802)が成功であれば、まず、この移動端末Xと外部網620の間のセッション用のIDを決定し、このセッションに利用するリンク情報650を決定する。

[0085]

そして、端末認証機能T A U T H 1は、認証応答パケットの内容をセッション情報管理テーブル（図15）の対応するフィールドに保存し、生成したセッションIDとリンク情報をもセッション情報管理テーブル（図15）の対応するフィールドに保存する。さらに、このとき端末認証機能T A U T H 1は、図12に示す認証応答パケットを生成し、端末に送信するため、チャネル多重分離機能C H MUX2へ出力する。

[0086]

図21のフローチャートを用いてセッション情報の転送手順の一部について説明する。

[0087]

イント制御管理機能A P M 1に出力する。

【0088】

また、セッション情報ハンドオーバー機能H O F 1は、別のアクセスポイントから図18に示すセッション情報通知パケット900を受信すると、移動端末I D 9 0 2、外部網I D 9 0 3、アクセスポイント-移動端末間認証用セキュリティアソシエーション904、セッションI D 9 0 5、リンク情報906をセッション情報管理テーブル（図15）に保存する。

【0089】

図20のフローチャートを用いてセッション情報の転送手順の一部について説明する。

【0090】

端末認証機能T A U T H 1は、移動端末Xからの認証要求パケット700に旧アクセスポイントI Dが設定されている場合は、前述の認証手順を行う代わりに、セッション情報ハンドオーバー機能H O F 1にこれを通知する。セッション情報ハンドオーバー機能H O F 1は図19に示すセッション情報ハンドオーバー要求パケット900を生成し、旧アクセスポイントに対して送信する。

【0091】

セッション情報ハンドオーバー機能H O F 1は、図19に示すセッション情報ハンドオーバー要求パケット1000を受信すると、前述の手順で図19に示すセッション情報ハンドオーバー通知パケットを送信する。

【0092】

なお、有線アクセスポイントの場合、無線送受信機T R 0 7 aが有線回線用の送受信機となる他は無線アクセスポイントと同じ構成であるため説明を省略する。

【0093】

図22に移動通信網認証サーバの構成を示す。移動通信網認証サーバM A S 1は、送受信機T R 0 8、仮想コア網多重分離機能C M U X M、端末認証機能T A U T H、外部網判定機能E D E C 1、ホーム認証サーバ通信機能H A S C 1から構成される。

## 【0094】

送受信機TR08は、コア網CNとの間でパケットの送受信を行う。

## 【0095】

仮想コア網多重分離機能CMUXMは、送受信機TR08から入力されたパケットを仮想コア網毎に分離し、外部網（1）用仮想コア網VCN1、外部網（2）用仮想コア網VCN2、外部網（3）用仮想コア網VCN3から受信したパケットは、ホーム認証サーバ通信機能HASC1へ出力し、制御管理用仮想コア網VCNSから受信したパケットを端末認証機能TAUTHへ出力する。

## 【0096】

また、ホーム認証サーバ通信機能HASC1から入力された外部網（1）用仮想コア網VCN1、外部網（2）用仮想コア網VCN2、外部網（3）用仮想コア網VCN3向けのパケットと、端末認証機能TAUTHから入力された管理制御用仮想コア網VCNS向けのパケットとを仮想網毎に多重し、送受信機能TR08へ出力する。

## 【0097】

図27に示すフローチャートを用いて端末認証関連のパケットの処理を説明する。

## 【0098】

端末認証機能TAUTHは、図23に示す端末情報管理テーブルを保持している。端末認証機能TAUTHは、無線アクセスポイントまたは有線アクセスポイントから受信した図16に示す認証要求パケット700を仮想コア網多重分離機能CMUXMから入力されると、図23の端末情報管理テーブルの端末ID1110と移動通信網-移動端末間セキュリティアソシエーション1120に基づき、このパケットを認証する。認証が成功すれば移動通信網において移動端末が認証されたことになる。

## 【0099】

また、このとき端末認証機能TAUTHは、外部網判定機能EDC1にホーム網IDに対応する外部網ID問い合わせる。外部網判定機能EDC1は、図24に示すホーム網-外部網対応テーブルを保持しており、これに基づき外部網I

D1220を返答する。さらに、このとき端末認証機能TAUTHはホーム網認証サーバ通信機能HASC1にホーム網への移動端末の認証を依頼する。

## 【0100】

これに対しホーム網認証サーバ通信機能HASC1は、図25に示す認証要求パケット1300を生成し、ホーム網の認証サーバに送信するため対応する外部網用仮想コア網を選択し、仮想コア網多重分離機能CMUXMへ出力する。

## 【0101】

これに対し、ホーム認証サーバはホーム網用移動端末IDとホーム網において保持しているホーム網一移動端末間セキュリティアソシエーションに基づきパケットを認証し、図26に示す認証応答パケット1400を返信する。

## 【0102】

ホーム網認証サーバ通信機能HASC1は、図26に示す認証応答パケット1400を仮想コア網多重分離機能CMUXMから入力されると、これを端末認証機能TAUTHへ出力する。この時点で移動端末は移動通信網とホーム網の両方に認証されたことになる。

## 【0103】

端末認証機能TAUTHは、アクセスポイントと移動端末間でパケットを認証するために使用するアクセスポイント一移動端末間セキュリティアソシエーションを作成し、図17に示す認証応答パケット800を生成し、アクセスポイントに送信するため仮想コア網多重分離機能CMUXMへ出力する。

## 【0104】

図28を用いて、これまでに説明してきた移動端末の認証の手順の流れの全体像を説明する。

## 【0105】

まず移動端末Xは、図11に示す認証要求パケット400を生成し、これを認証用チャネルM01を介してアクセスポイントAPa1へ送信する。

## 【0106】

これを受信したアクセスポイントAPa1は、図16に示す認証要求パケット700を生成し、これを制御管理用アクセス網VANaSを介して移動通信網認

証サーバMASへ送信する。途中、アクセス網ゲートウェイAGWaが制御管理用仮想アクセス網VANaSから受信したパケットを制御管理用仮想コア網VCNSへ転送する。

## 【0107】

これを受信した移動通信網認証サーバMASは、移動端末の認証を行うと共に、図25に示す認証要求パケットを1300生成し、これを先のホーム網に応答する外部網用仮想コア網VCN1を介してホーム認証サーバHAS1へ送信する。途中、外部網ゲートウェイTGW1が外部網用仮想コア網VCN1から受信したパケットを外部網(1)EX1へ転送する。

## 【0108】

これを受信したホーム網認証サーバHASは、移動端末の認証を行うと共に、図26に示す認証応答パケット1400を生成し、これを移動通信網認証サーバMASへ送信する。途中、外部網ゲートウェイTGW1は、外部網EX1から受信したパケットを外部網用仮想コア網VCN1へ転送する。

## 【0109】

これを受信した移動通信網認証サーバMASは、アクセスポイント-移動端末間セキュリティアソシエーションを生成すると共に、図17に示す認証応答パケット800を生成し、これを制御管理用仮想コア網VCNSを介してアクセスポイントAPa1へ送信する。途中、アクセス網ゲートウェイAGWaが制御管理用仮想コア網VCNSから受信したパケットを制御管理用仮想アクセス網VANaSへ転送する。

## 【0110】

これを受信したアクセスポイントAPa1は、アクセスポイント-移動端末間セキュリティアソシエーション506を保存し、セッションID507と対応するリンク情報508を生成するとともに、図12に示す認証応答パケット500を生成し、これを認証用チャネルを介して移動端末Xへ送信する。

## 【0111】

これを受信した移動端末Xは、アクセスポイント-移動端末間セキュリティアソシエーション506と、セッションID507と対応するリンク情報508を

保存する。

【0112】

以上の手順を経て、移動端末と移動通信網、ホーム網との端末認証が終了し、移動端末とアクセスポイント間には外部網と通信するためのセッションとそのためのリンク情報とセキュリティアソシエーションが設定される。

【0113】

図29に基づき、端末認証後のパケットの送信と受信の流れを説明する。

【0114】

まず、移動端末X上のホーム網毎の通信エンティティENT1がパケットを送信する場合、ホーム網に対応するセッションが選択される。そしてそのセッション用のリンク情報を用いて、パケットは通信用チャネルCH1上をアクセスポイントAPa1へ送信される。

【0115】

アクセスポイントAPa1では、まず受信したパケットのパケット認証を行う。そしてパケットの属するセッションに対応した外部網、この場合、外部網(1)、が選択され、その外部網用の仮想アクセス網、この場合、VANa1、上へパケットは出力される。

【0116】

このパケットは通信相手が同じ仮想アクセス網配下にいる場合は、その通信相手が接続しているアクセスポイントへ転送される。また、通信相手が別のアクセス網配下もしくは外部網にいる場合は、このパケットはアクセス網ゲートウェイAGWaを介して、仮想アクセス網、この例ではVANa1、に対応する仮想コア網、この例ではVCN1、へ出力される。

【0117】

さらに、このパケットは通信相手が別のアクセス網配下にいる場合は、仮想コア網、この例ではVCN1、を介して、そのアクセス網ゲートウェイへ転送される。また、通信相手が外部網にいる場合は、このパケットは外部網ゲートウェイ、この例ではEGW1、を介して、外部網へ出力される。

【0118】

次に移動端末がパケットを受信する場合の流れを示す。

【0119】

外部網（1）EX1からパケットが到着した場合は、そのパケットは対応する仮想コア網上VCN1を転送される。このパケットは、現在、移動端末がいるアクセスマッシュのアクセスマッシュゲートウェイAGWaを介して、対応する仮想アクセスマッシュ上VANa1を転送される。そして、アクセスポイントAPa1がある外部網用の仮想アクセスマッシュ上からパケットを受信すると、その外部網とパケットのあて先の移動端末のIDとからセッションが選択される。

【0120】

そして、パケットにはパケット認証コードが付加され、セッションに対応したリンク情報を用いてパケットは通信用チャネルCH1上を移動端末Xへ送信される。

【0121】

移動端末Xはパケットを受信するとパケット認証を行い、パケットが属するセッションに基づき適切なホーム網との通信エンティティへパケットを渡す。

【0122】

図30に一例として外部網EX1に移動管理ノードMA1が配置されている場合の、移動端末Xの位置登録の手順を示す。これはモバイルIPなどの既存の技術を用いて行われるため概要のみを示す。位置登録要求パケットM30は、前述のパケットの流れに従って移動管理ノードMA1へ送信される。

【0123】

これを受信すると、移動管理ノードMA1は端末の位置を保持した上で、位置登録応答パケットM31を移動端末Xへ返信する。他の端末からこの移動端末宛に送信されたパケットはまず、移動管理ノードMA1へ届き、移動管理ノードはこれを登録された位置情報に基づき移動端末Xへ転送する。

【0124】

図31と図32に移動端末があるアクセスポイントから他のアクセスポイントにハンドオーバーする場合の手順を示す。

【0125】

ハンドオーバーの形態としては、（1）移動端末が新たなアクセスポイントへハンドオーバーすることを決定し、現在接続されている古いアクセスポイントに対して新たなアクセスポイントを通知する形態、（2）移動端末が接続されているアクセスポイントが、移動端末がハンドオーバーすべき新たなアクセスポイントを決定し、移動端末にこれを通知する形態、（3）移動端末が新たなアクセスポイントに接続してから、新たなアクセスポイントに以前接続されていた古いアクセスポイントを通知する形態、の3つがある。

## 【0126】

図31はこのうち最初の2つの手順の場合を示す。旧アクセスポイントAPoが移動端末Xのハンドオーバー先の新アクセスポイントAPnを自ら決定する場合、あるいは移動端末Xからハンドオーバー先の新アクセスポイントAPn通知された場合、移動前の旧アクセスポイントAPoはセッション情報テーブルからこの移動端末の全てのセッション情報を取り出し、図18に示すセッション情報ハンドオーバー通知パケットを作成し、これを移動後の新アクセスポイントAPnへ送信する。

## 【0127】

このとき、新アクセスポイントが別のアクセス網配下にある場合、アクセス網GWを介してパケットは転送される。新アクセスポイントAPnはこの情報をセッション管理情報テーブルに設定する。

## 【0128】

また、図32は上記の3つのハンドオーバーの形態のうち3番目の場合の手順を示す。移動後の新アクセスポイントAPnは、移動端末からの図11に示す認証要求パケットを受信すると、これに設定されている旧アクセスポイントIDに基づき、移動前の旧アクセスポイントAPoへ図19に示すセッション情報ハンドオーバー要求を送信する。

## 【0129】

旧アクセスポイントAPoは、セッション情報テーブルからこの移動端末の全てのセッション情報を取り出し、図18に示すセッション情報ハンドオーバー通知パケットを作成し、これを移動後の新アクセスポイントAPnへ送信する。新

アクセスポイントはこの情報をセッション管理情報テーブルに設定する。

#### 【0130】

以上の手順により、移動端末は他のアクセスポイント配下に移動した場合、同じ外部網との通信を継続することができる。

#### 【0131】

(第2の実施の形態)

図33を用いて、本発明の第2の実施の形態について説明する。図33の移動通信網の構成は図1と殆ど同じであり、違いはコア網にローカル移動管理ノードLMA1が追加されている点だけである。

#### 【0132】

図34はローカル移動管理ノードLMA1の構成を示す。ローカル移動管理ノードLMA1は、送受信機TR09、仮想コア網多重分離機能CMUXL、外部網(1)用仮想ローカル移動管理ノードVLMA1、外部網(2)用仮想ローカル移動管理ノードVLMA2、外部網(3)用仮想ローカル移動管理ノードVLMA3、制御管理用仮想ローカル移動管理ノードVLMAS、から構成される。

#### 【0133】

送受信機TR09は、コア網CNと接続され、パケットの送受信を行う。

#### 【0134】

仮想コア網多重分離機能CMUXLは、コア網側送受信機TR09から入力されたパケットを仮想コア網毎に分離し、外部網(1)用仮想コア網VCN1から受信したパケットは外部網(1)用仮想ローカル移動管理ノードVLMA1に出力し、外部網(2)用仮想コア網VCN2、外部網(3)用仮想コア網VCN3、管理制御用仮想コア網VCNSについても同様の処理を行う。

#### 【0135】

また、仮想コア網多重分離機能CMUXLは、外部網(1)用仮想ローカル移動管理ノードVLMA1から入力されたパケットを外部網(1)用仮想コア網上VCN1に出力し、外部網(2)用仮想ローカル移動管理ノードVLMA2、外部網(3)用ローカル移動管理ノードVLMA3、制御管理用仮想ローカル移動管理ノードVLMASについても同様の処理を行い、各仮想コア網を多重して、

送受信機TR09に出力する。

【0136】

個々の仮想ローカル移動管理ノードは、Mobile IP等の既存技術を使用している。図35を用いて、この手順を説明する。移動端末Xは、外部網(1)用仮想ローカル移動管理ノードVLMA1へ位置登録要求を送信する。これを受信した、外部網(1)用仮想ローカル移動管理ノードVLMA1は移動端末の位置情報を保持し、位置登録応答を送信する。

【0137】

また、移動端末X宛のパケットが送られてくると、外部網(1)用仮想ローカル移動管理ノードVLMA1はこのパケットを移動端末Xから通知された位置へ転送する。これにより仮想網上で端末の移動をサポートする機能を提供する。

【0138】

以上好ましい実施の形態及び実施例をあげて本発明を説明したが、本発明は必ずしも上記実施の形態及び実施例に限定されるものではなく、その技術的思想の範囲内において様々に変形して実施することができる。

【0139】

【発明の効果】

以上説明したように本発明によれば、次に述べるような効果が実現される。

【0140】

従来技術では移動端末で通信を行う場合、パケットは外部網ゲートウェイを介して転送されていた。これに対して、本発明では移動端末間で通信を行う場合、同一アクセスポイント配下に各移動端末がいるときは、アクセスポイントで折り返して通信を行い、同一アクセス網配下に各移動端末がいるときは、アクセス網を介して通信を行い、別のアクセス網配下に各移動端末がいるときは、コア網を経由して通信を行うこととなり、コア網、アクセス網の回線使用効率が改善される。

【0141】

また、マルチキャストの通信に関しても従来技術では外部網ゲートウェイにおいてマルチキャストパケットを受信する移動端末の数だけマルチキャストパケッ

トがコピーされ移動端末へのトンネル上を転送されていたため回線利用効率が悪かったが、本発明ではコア網やアクセス網上のパケットはマルチキャストを使用して転送されるため効率が改善される。

## 【0142】

また、本発明によれば、仮想コア網、仮想アクセス網がプライベート網を形成するため、移動端末間でセキュリティアソシエーションを確立する手間が不要となる。

## 【0143】

さらに、本発明によれば、移動通信網上のノード間の通信も制御管理用の仮想コア網、仮想アクセス網により保護されるため、ノード間でセキュリティアソシエーションを確立する手間が不要となる。

## 【0144】

さらに、本発明によれば、移動端末がハンドオーバーする際に移動端末と外部網との専用線接続が途切れることなく継続できる。

## 【図面の簡単な説明】

【図1】 本発明の第1の実施の形態による網全体の構成を示す図である。

【図2】 本発明の第1の実施の形態におけるコア網とその上に多重される仮想コア網の関係を示す図である。

【図3】 本発明の第1の実施の形態におけるコア網とその上に多重される仮想アクセス網の関係を示す図である。

【図4】 本発明の第1の実施の形態における無線及び有線ドロップ回線とその上に多重される認証用チャネルと通信用チャネルの関係、及び通信用チャネル上に多重される移動端末と外部網間のセッションの関係を示す図である。

【図5】 本発明の第1の実施の形態における外部網ゲートウェイの構成を示す図である。

【図6】 本発明の第1の実施の形態におけるアクセス網ゲートウェイの構成を示す図である。

【図7】 本発明の第1の実施の形態における移動端末の構成を示す図である。

【図8】 移動端末が保持する移動通信網情報管理テーブルの構成を示す図である。

【図9】 移動端末が保持するホーム網情報管理テーブルの構成を示す図である。

【図10】 移動端末が保持するセッション情報管理テーブルの構成を示す図である。

【図11】 移動端末がアクセスポイントに送信する認証要求パケットの内容を示す図である。

【図12】 アクセスポイントが移動端末に送信する認証応答パケットの内容を示す図である。

【図13】 端末認証の手順を示すフローチャートである。

【図14】 アクセスポイントの構成を示す図である。

【図15】 アクセスポイントのセッション情報管理テーブルの構成を示す図である。

【図16】 アクセスポイントが移動通信網認証サーバに送信する認証要求パケットの内容を示す図である。

【図17】 移動通信網認証サーバがアクセスポイントに送信する認証応答パケットの内容を示す図である。

【図18】 旧アクセスポイントが新アクセスポイントに送信するセッション情報通知パケットの内容を示す図である。

【図19】 新アクセスポイントが旧アクセスポイントに送信するセッション情報要求パケットの内容を示す図である。

【図20】 アクセスポイントにおける端末認証関連のパケットの処理を示すフローチャートである。

【図21】 アクセスポイントにおけるセッション情報ハンドオーバー通知パケットの送信処理を示すフローチャートである。

【図22】 移動通信網認証サーバの構成を示す図である。

【図23】 移動端末管理情報テーブルの構成を示す図である。

【図24】 ホーム網一外部網対応テーブルの構成を示す図である。

【図25】 移動通信網認証サーバがホーム網認証サーバに送信する認証要求パケットの内容を示す図である。

【図26】 ホーム網認証サーバが移動通信網認証サーバに送信する認証応答パケットの内容を示す図である。

【図27】 移動網認証サーバにおける端末認証の手順を示すフローチャートである。

【図28】 端末認証の手順を示す図である。

【図29】 パケットの送受信の流れを示す図である。

【図30】 ホーム網の移動管理ノードへの位置登録の流れを示す図である

【図31】 旧アクセスポイントから新アクセスポイントへセッション情報を転送する手順を示す図である。

【図32】 新アクセスポイントから旧アクセスポイントへセッション情報の転送を要求する手順を示す図である。

【図33】 本発明の第2の実施の形態における全体構成を示す図である。

【図34】 本発明の第2の実施の形態におけるローカル移動管理ノードの構成を示す図である。

【図35】 ローカル移動管理ノードへの位置登録の手順を示す図である。

#### 【符号の説明】

E X n 外部網 (n)

M N W 移動通信網

C N コア網

M A n 移動管理ノード (n)

H A S n ホーム網認証サーバ (n)

E G W n 外部網ゲートウェイ (n)

M A S 移動通信網認証サーバ

A G W a アクセス網ゲートウェイ (a)

A N a アクセス網 (a)

A P a n 無線アクセスポイント (a - n)

X, Y, Z 移動端末

LMA 1 ローカル移動管理ノード

VCN n 外部網 (n) 用仮想コア網

VCS N 制御管理用仮想コア網

VAN a n 外部網 (n) 用仮想アクセス網 (a)

VAN a S 制御管理用仮想アクセス網 (a)

S a n 移動端末 (a) の外部網 (n) とのセッション

CH 1 通信用チャネル

CH 2 認証用チャネル

LD 有線ドロップ回線、または無線ドロップ回線

EGW n 外部網ゲートウェイ (n)

EGF 外部網ゲートウェイ機能

EGCF 外部網ゲートウェイ管理機能

CMUX 1 仮想コア網多重分離機能

TR 0 1 外部網側送受信機

TR 0 2 コア網側送受信機

AMUX 1 a 仮想アクセス網多重分離機能

TR 0 3 a コア網側送受信機

TR 0 4 a 外部網側送受信機

ANG a アクセス網ゲートウェイ (a)

VAGW n a 外部網 (n) 用仮想アクセス網ゲートウェイ (a)

VAGWS a 制御管理用仮想アクセス網ゲートウェイ (a)

ENT n ホーム網 (n) との通信エンティティー

TAUTH 2 端末認証機能 (移動端末)

SMUX セッション多重分離機能

CHMUX 1 チャネル多重分離機能 (移動端末)

PAUTH 1 パケット認証機能 (移動端末)

TR 0 5 無線送受信機 (移動端末)

TCH 通信用チャネル (移動端末)

C C H 認証用チャネル（移動端末）

T A U T H 1 端末認証機能

M A P 1 セッション外部網マッピング機能

S M T 1 セッション情報管理テーブル

A P M 1 アクセスポイント制御管理機能

A M U X 2 a 仮想アクセス網多重分離機能

H O F 1 セッション情報ハンドオーバ機能

P A U T H 2 パケット認証機能

C H M U X 2 チャネル多重分離機能

T R 0 6 a アクセス網側送受信機

T R 0 7 a 無線送受信機

E D E C 1 外部網判定機能

T A U T H 端末認証機能

H A S C 1 ホーム網認証サーバ通信機能

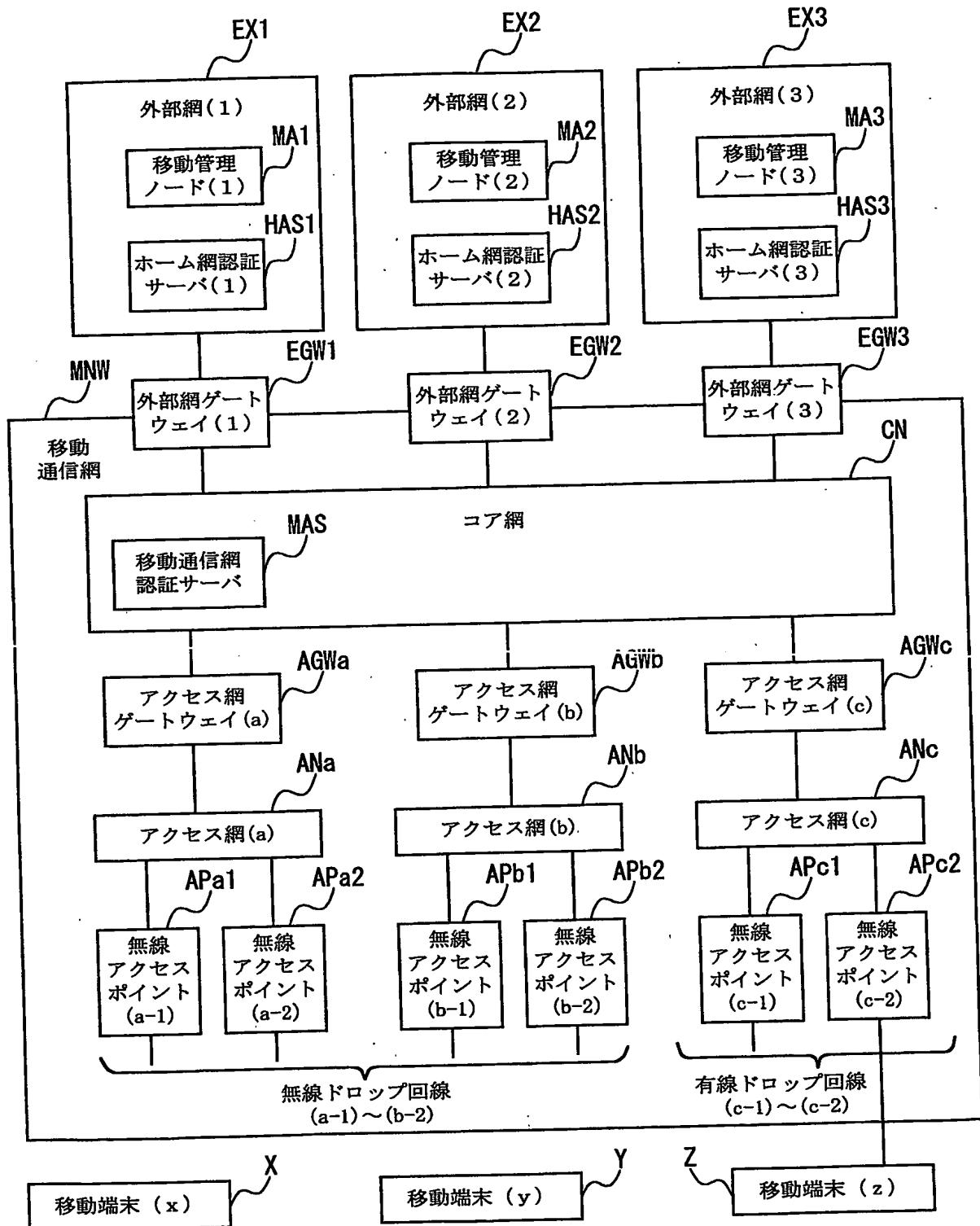
C M U X M 仮想コア網多重分離機能

T R 0 8 送受信機

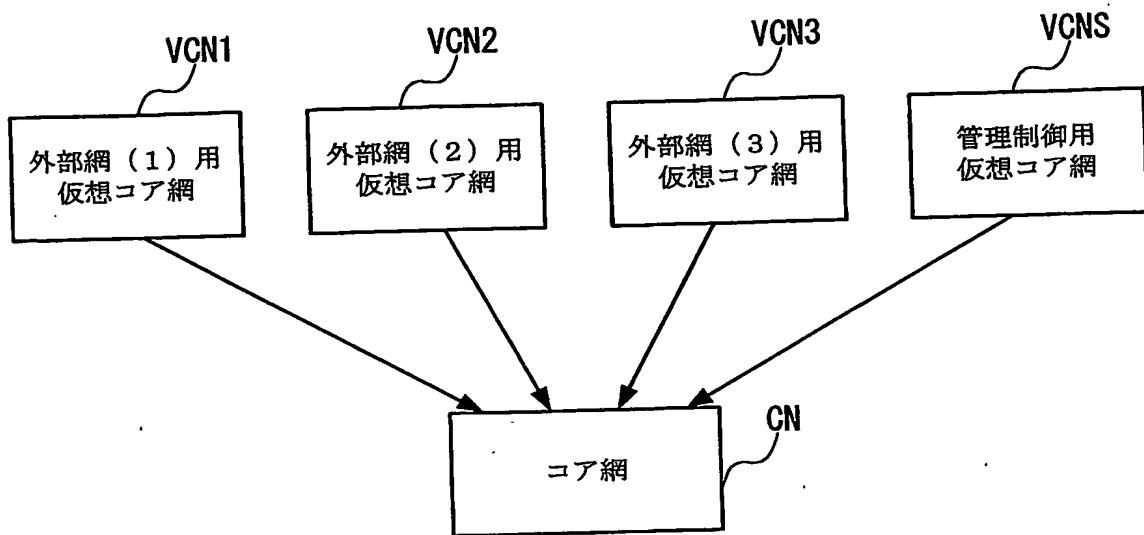
L M A 1 ローカル移動管理ノード

【書類名】 図面

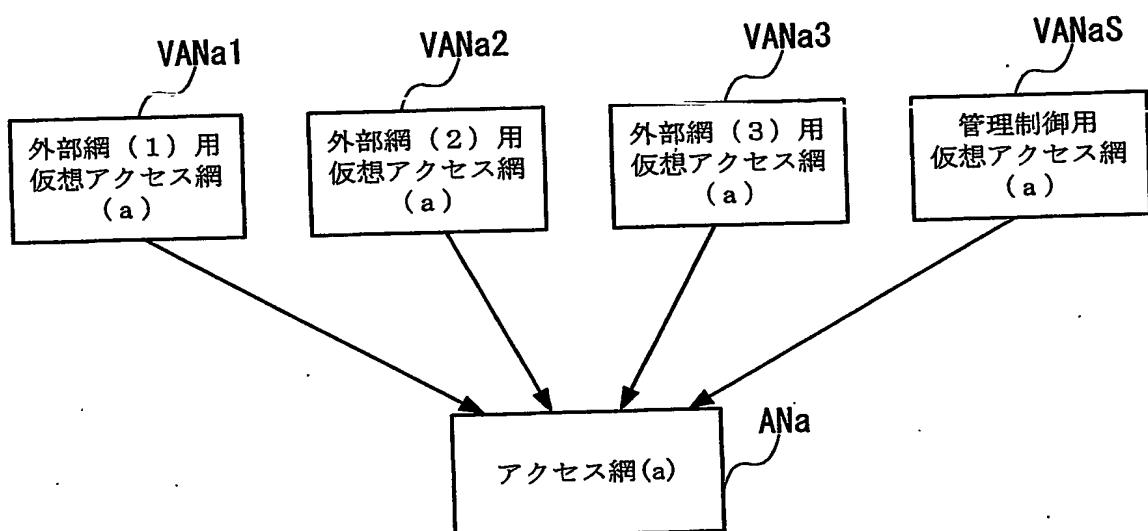
【図1】



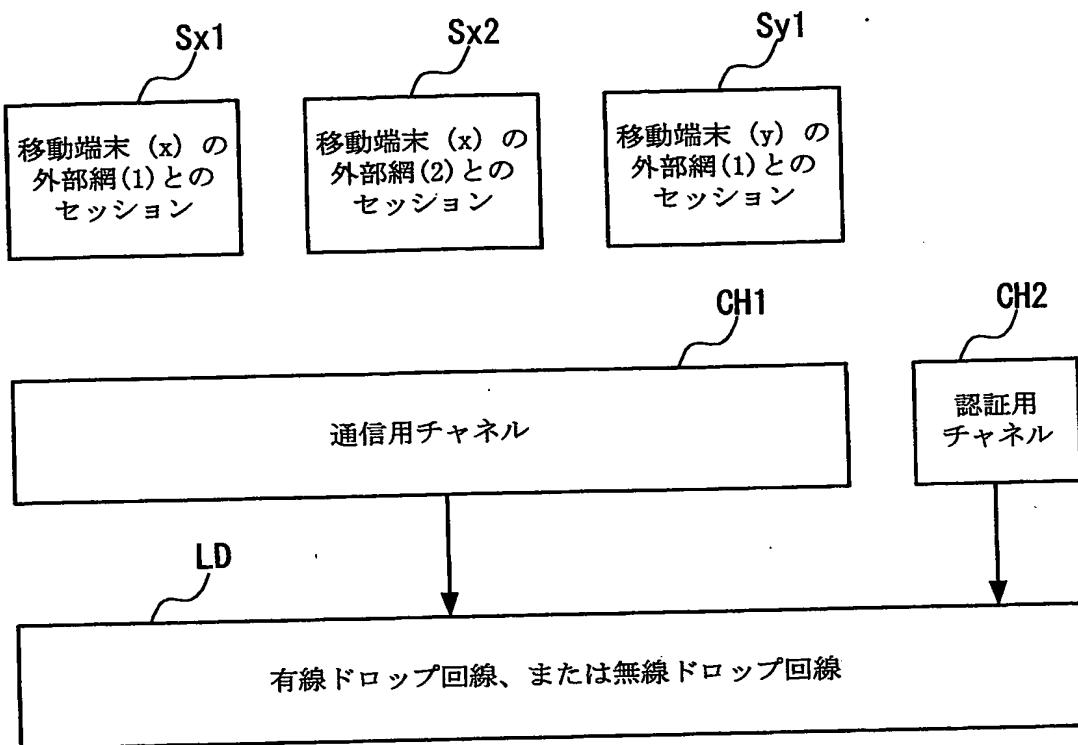
【図2】



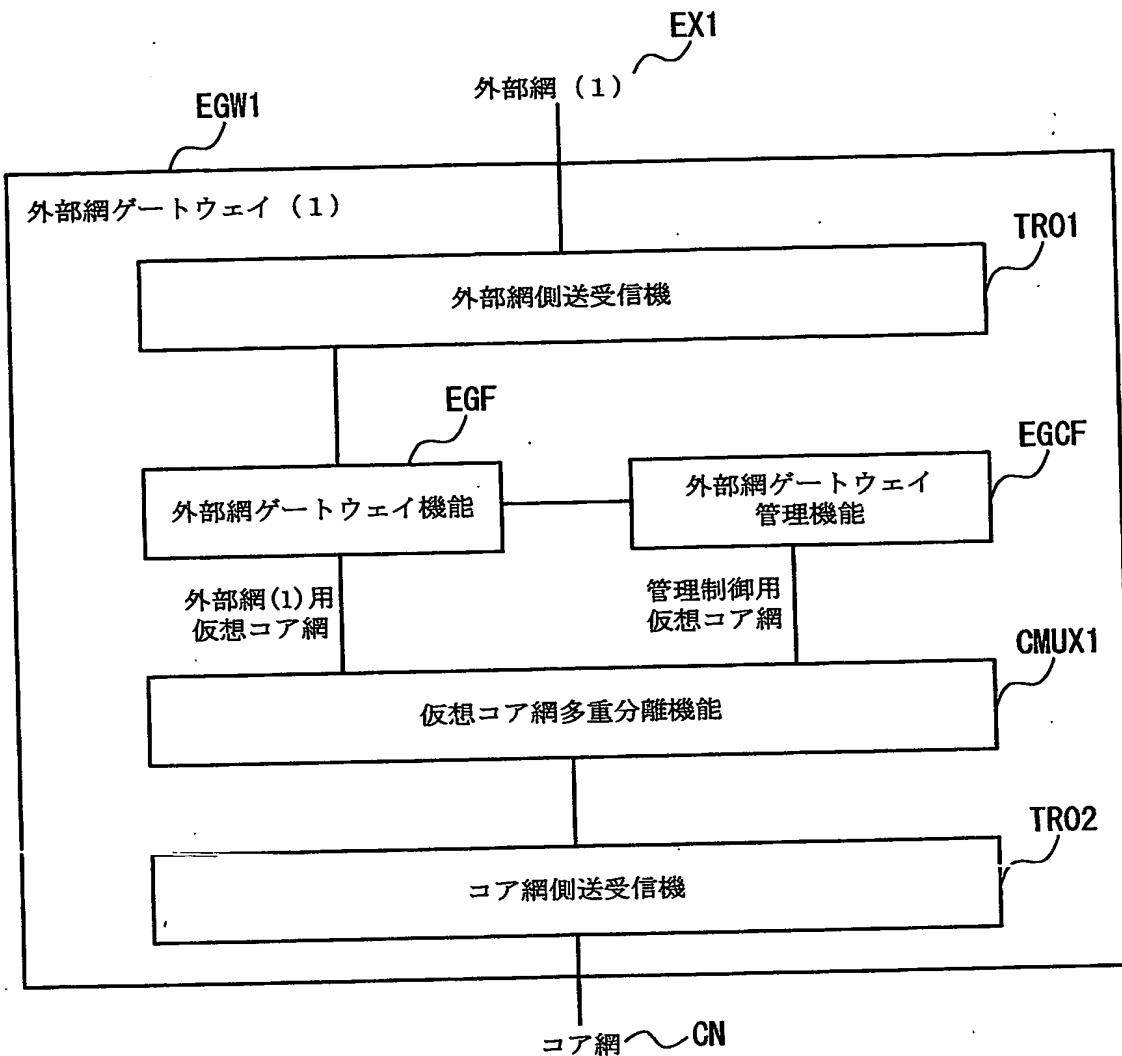
【図3】



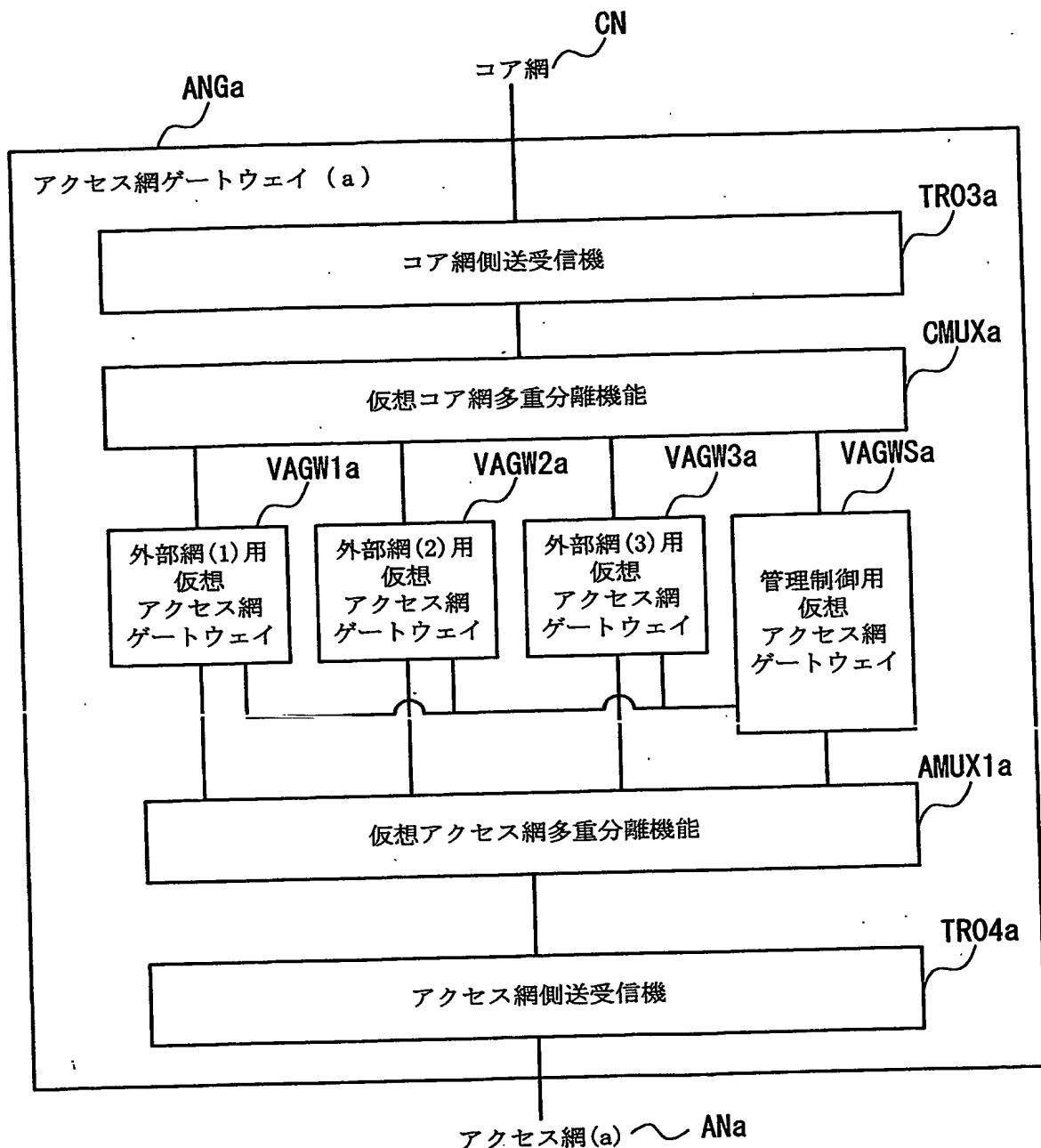
【図4】



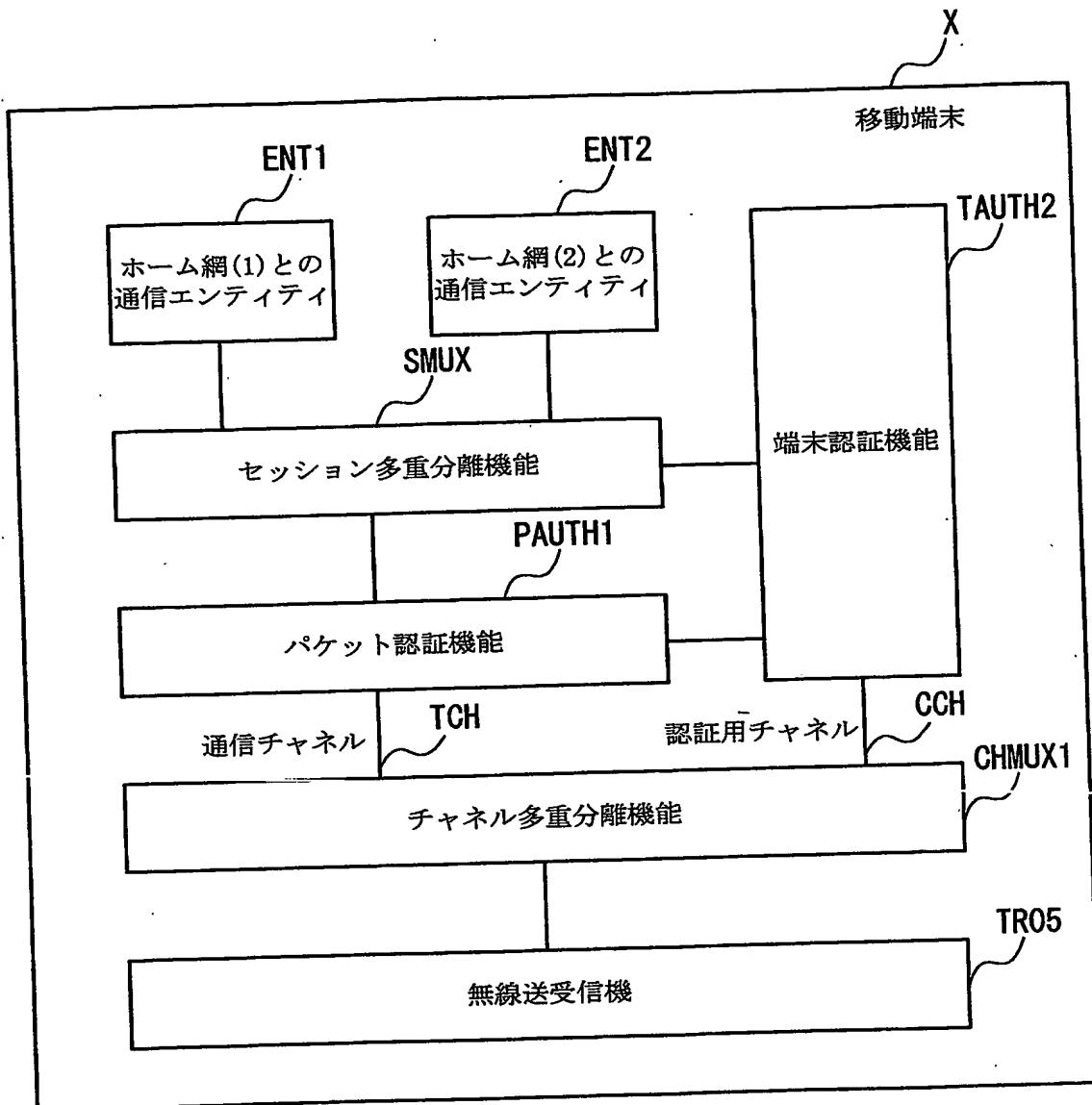
【図5】



【図6】



【図7】



【図8】

移動通信網情報管理テーブル

端末 I D	110
移動通信網-移動端末間セキュリティアソシエーション(SA)	111

【図9】

200 ホーム網情報管理テーブル

210	ホーム網 ID	ホーム網用 移動端末 ID	220	ホーム網認証サー バ ー移動端末間 SA	230
211	ホーム網 # 1	ID # 1 221		Home SA # 1 231	
212	ホーム網 # 2	ID # 2 222		Home SA # 2 232	

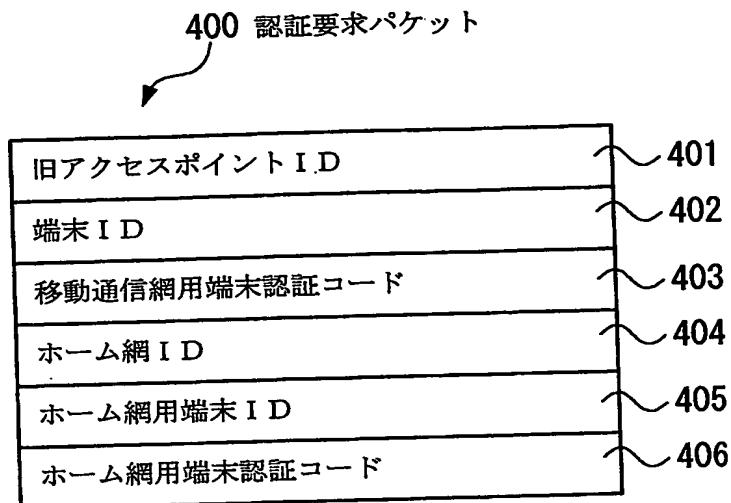
【図10】

300 セッション情報管理テーブル

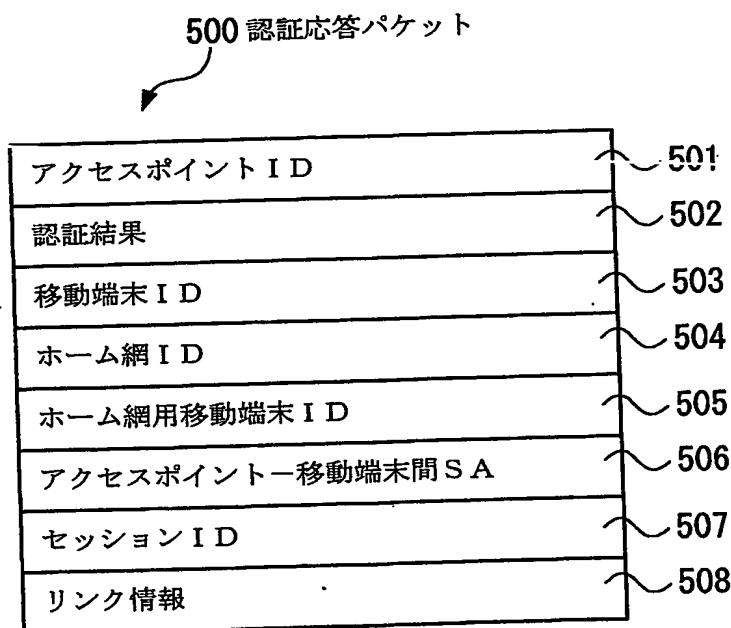
310	ホーミング ID	320	アクセス ポイント ID	330	アクセス ポイント -端末間SA	340	セッション ID	350	リンク情報
311	ホーム網 # 1	AP#1		AP-SA#1		S-ID#1		LINK#1	
312	ホーム網 # 2	AP#1		AP-SA#2		S-ID#2		LINK#2	

322 321 332 331 342 341 352 351

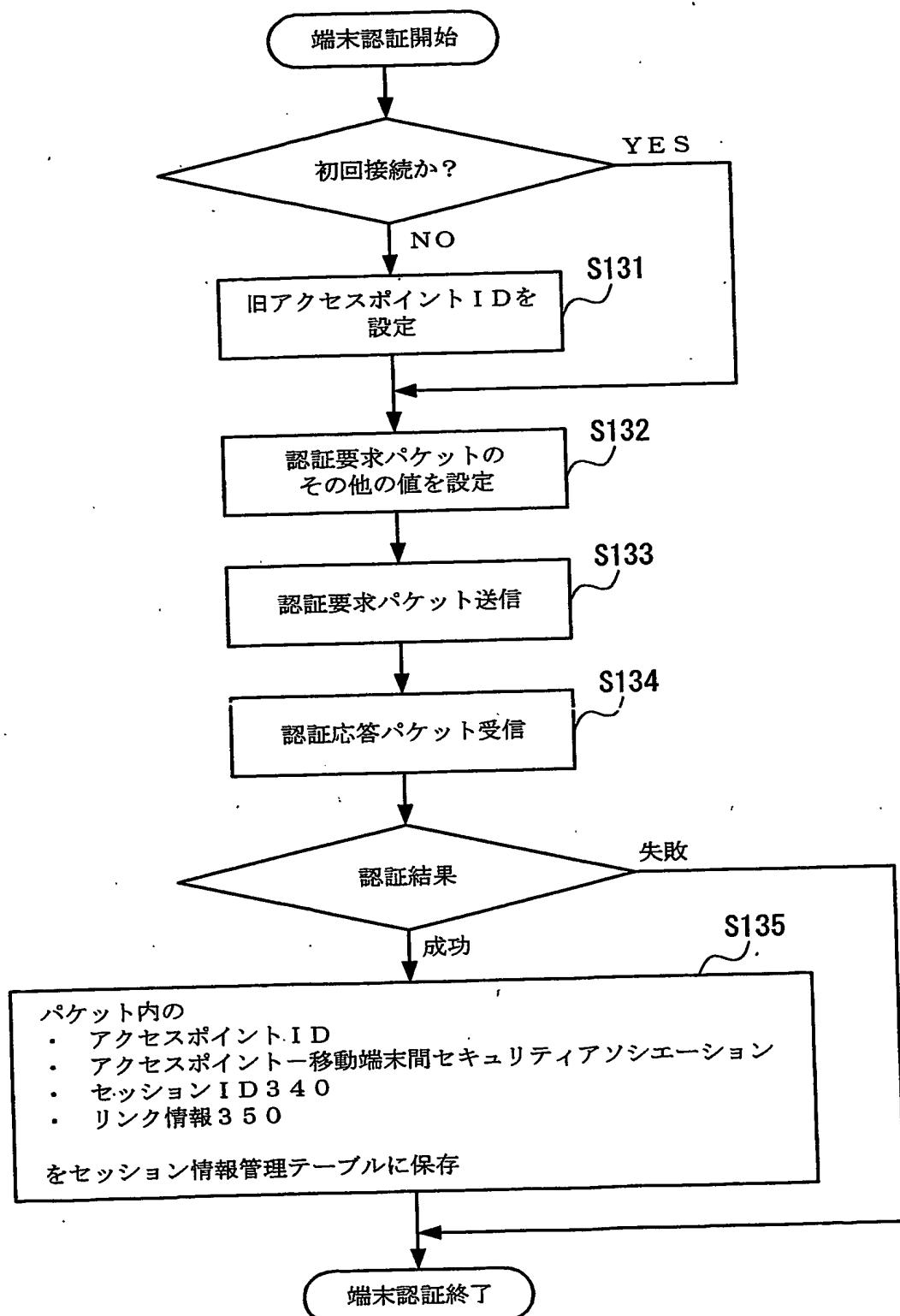
【図11】



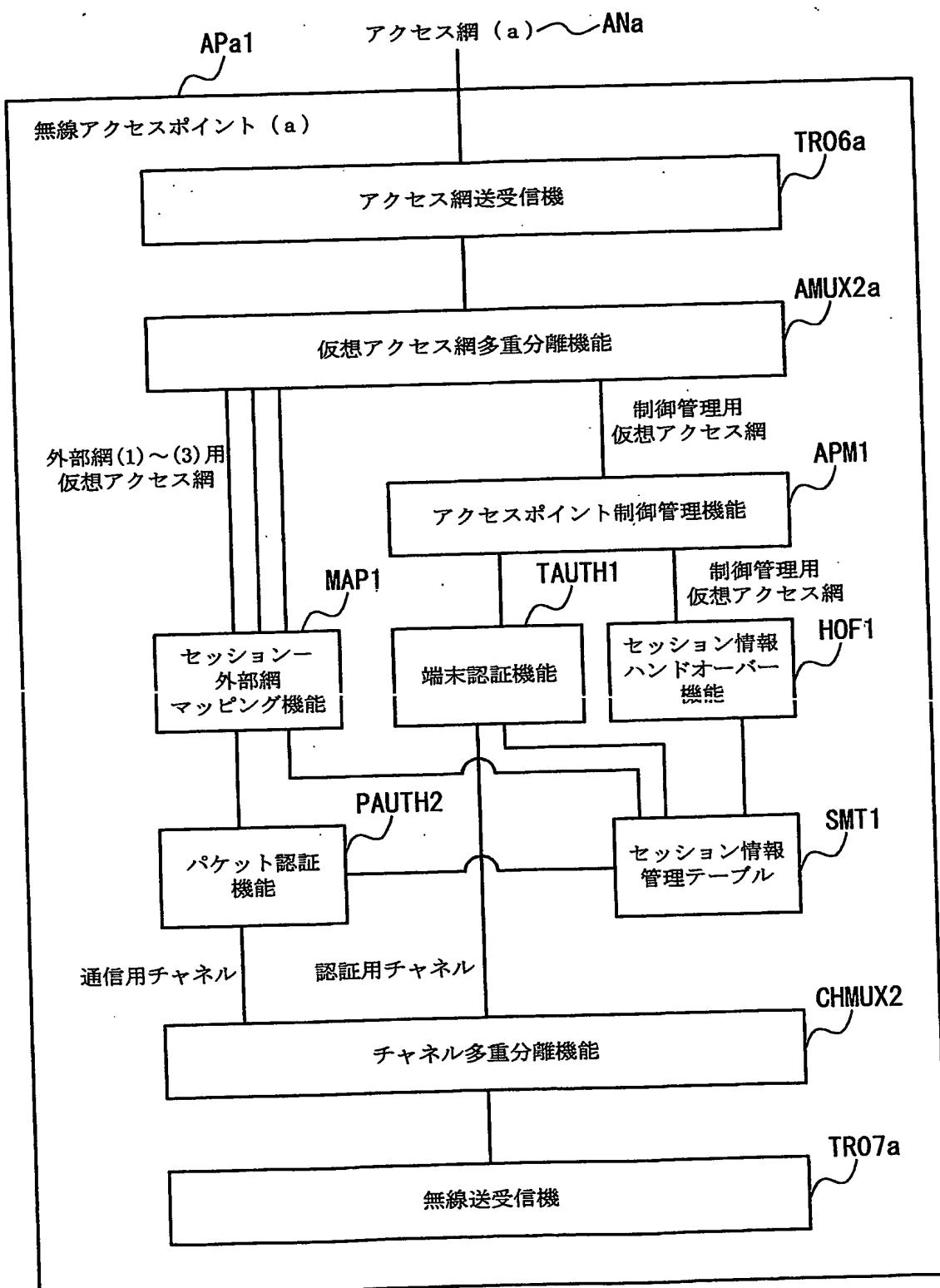
【図12】



【図13】



【図14】



【図15】

600 セッション情報管理テーブル

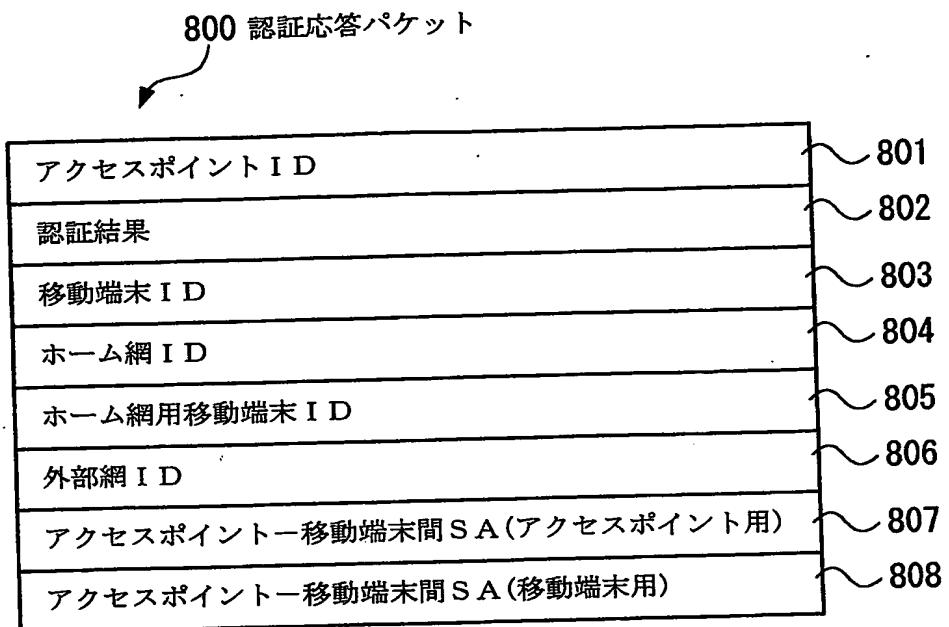
移動端末 I D 610	外部網 I D 620	アクセスポイントー 移動端末間 SA 630	セッション I D 640	リンク情報 650
移動端末 # 1 611	外部網 # 1 621	SA # 1 631	セッション # 1 641	リンク情報 # 1 651
移動端末 # 1 612	外部網 # 2 622	SA # 2 632	セッション # 2 642	リンク情報 # 2 652
移動端末 # 2 613	外部網 # 1 623	SA # 1 633	セッション # 1 643	リンク情報 # 1 653

【図16】

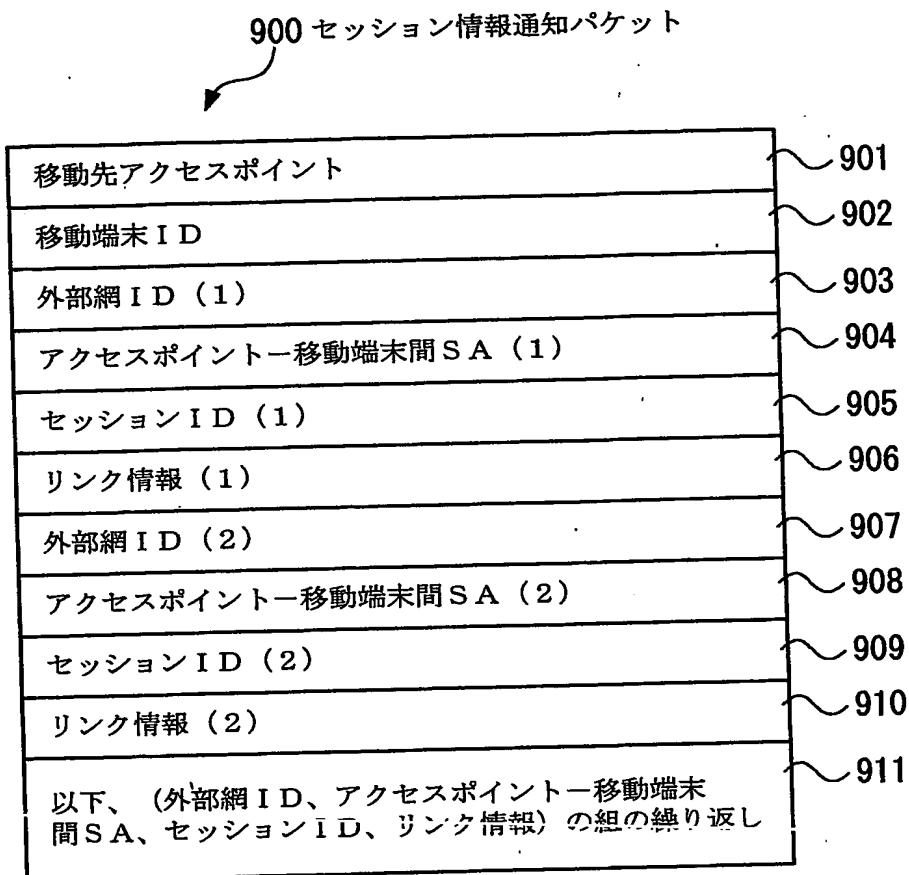
700 認証要求パケット

アクセスポイント I D	701
移動端末 I D	702
移動網用移動端末認証コード	703
ホーム網 I D	704
ホーム網用移動端末 I D	705
ホーム網用移動端末認証コード	706

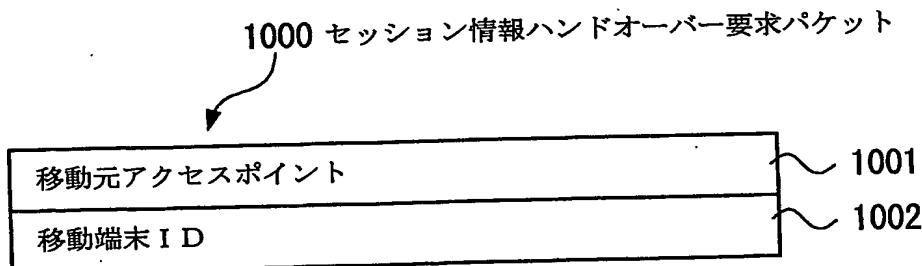
【図17】



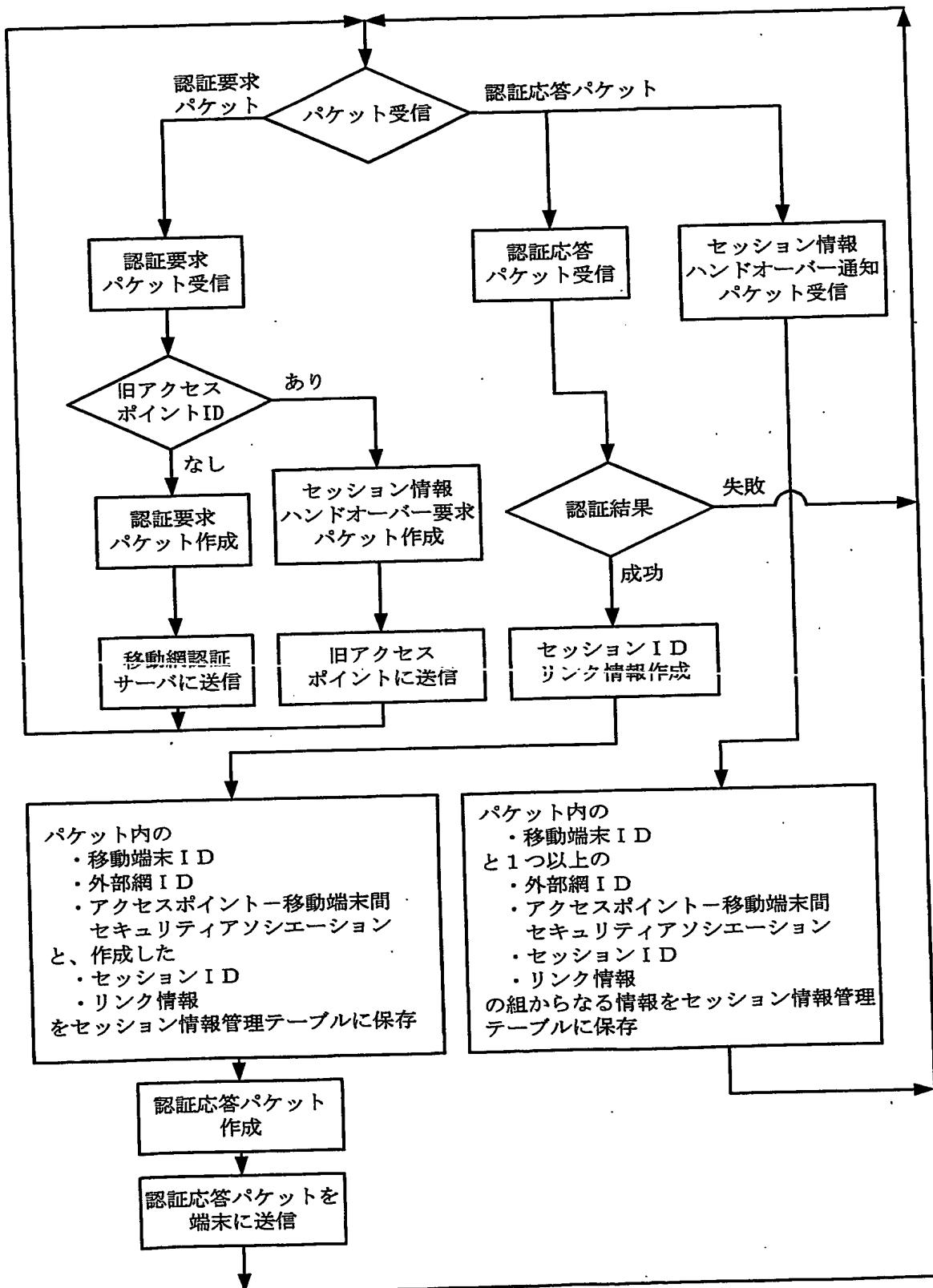
【図18】



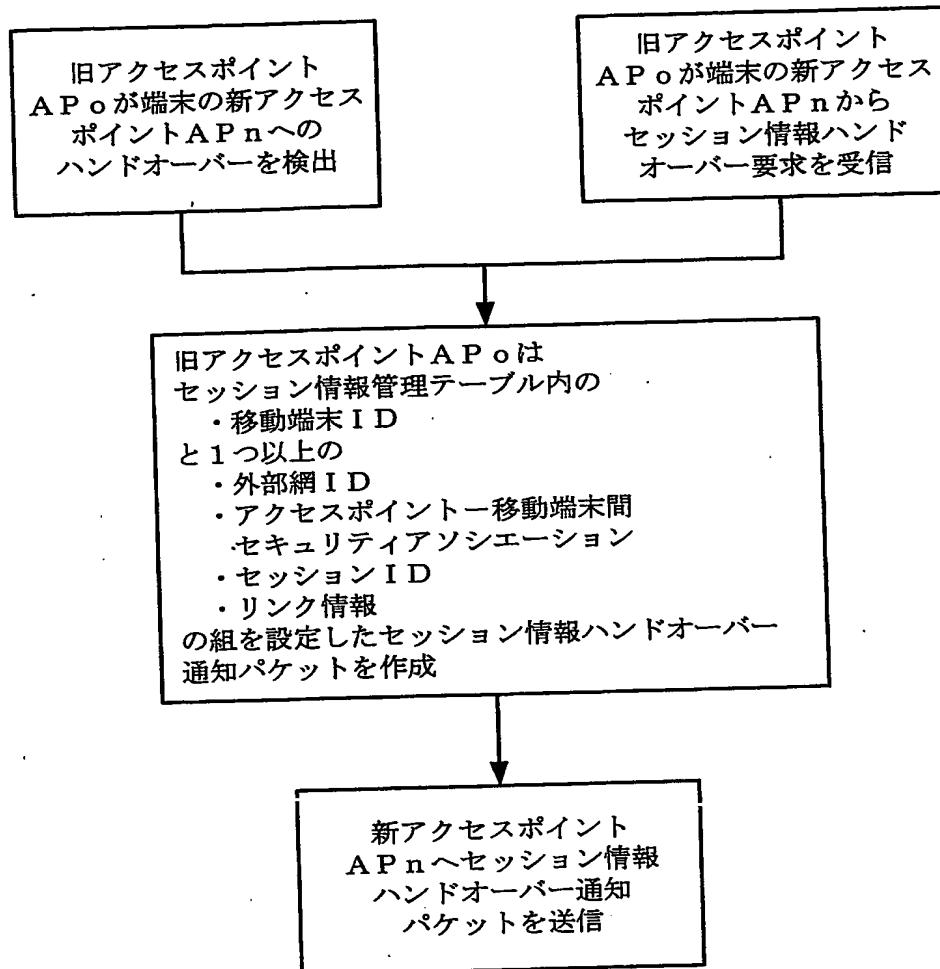
【図19】



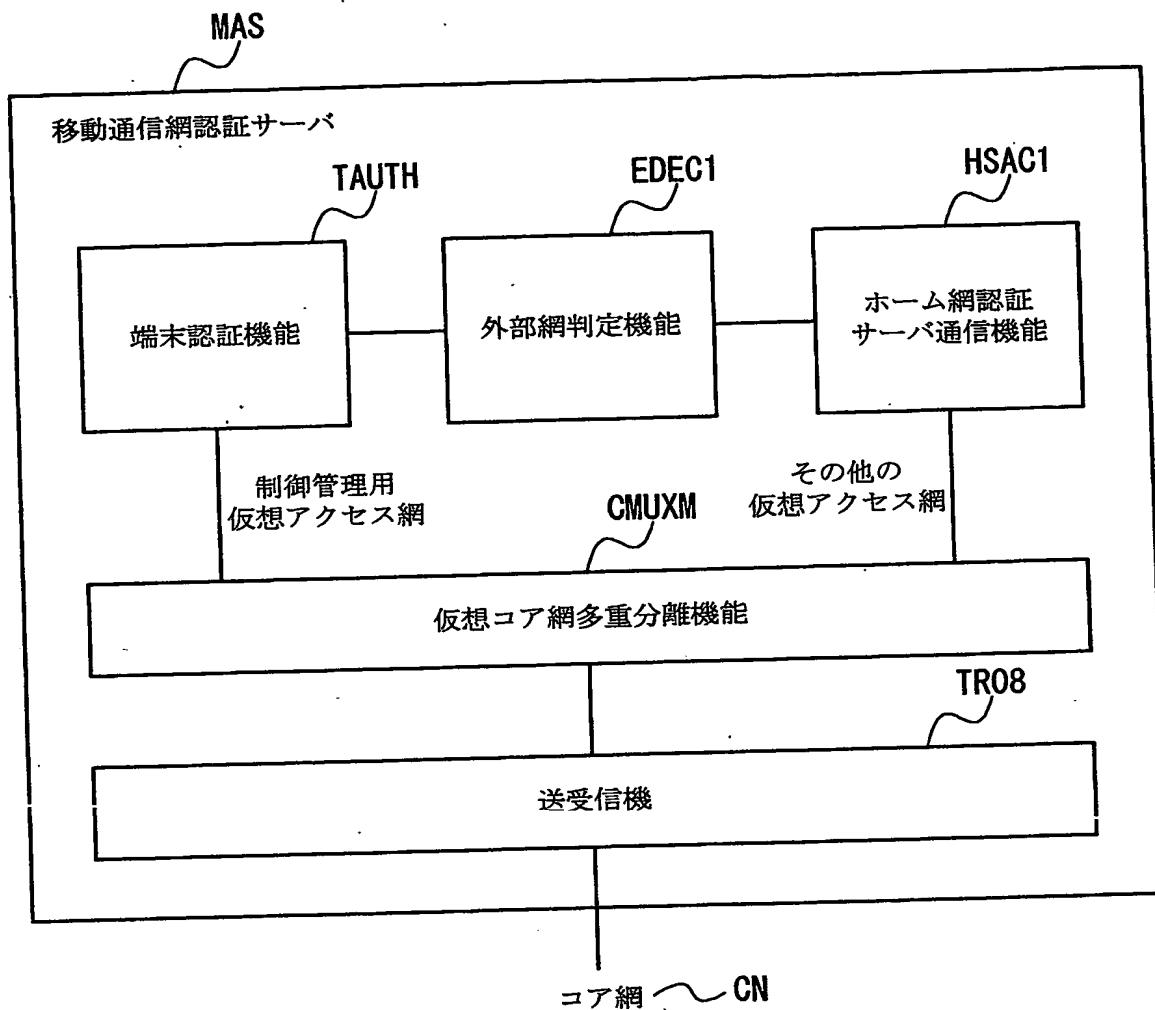
【図20】



【図21】



【図22】



【図23】

1100 端末情報管理テーブル

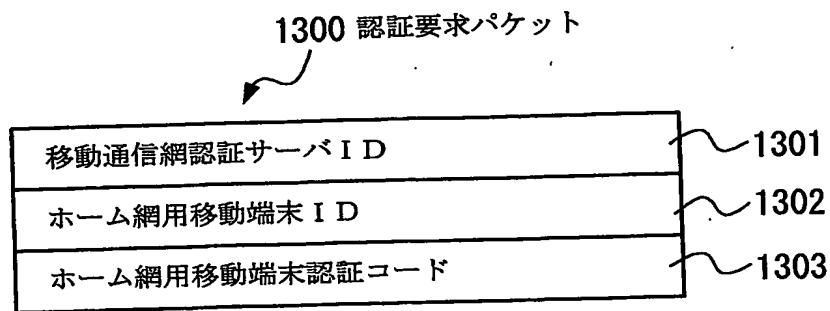
移動端末 I D (1110)	移動通信網認証サーバ —移動端末間 SA (1120)	アクセスポイント —移動端末間 SA (1130)
移動端末 # 1 (1111)	Home SA# 1 (1121)	SA# 1 (1131)
移動端末 # 2 (1112)	Home SA# 2 (1122)	SA# 2 (1132)

【図24】

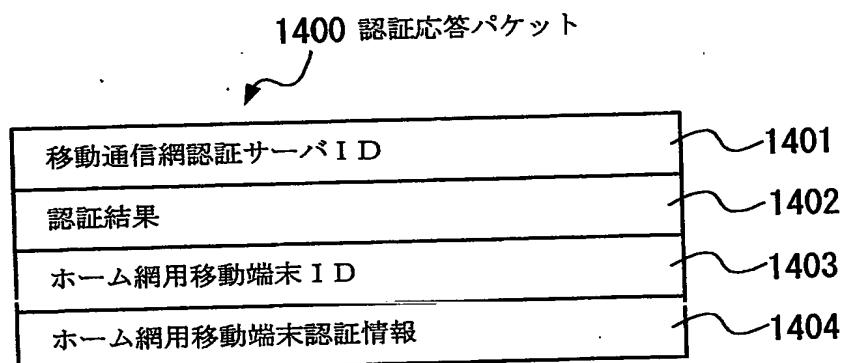
1200 ホーム網—外部網対応テーブル

ホーム網 I D (1210)	外部網 I D (1220)
ホーム網 # 1 (1211)	外部網 # 1 (1221)
ホーム網 # 2 (1212)	外部網 # 2 (1222)

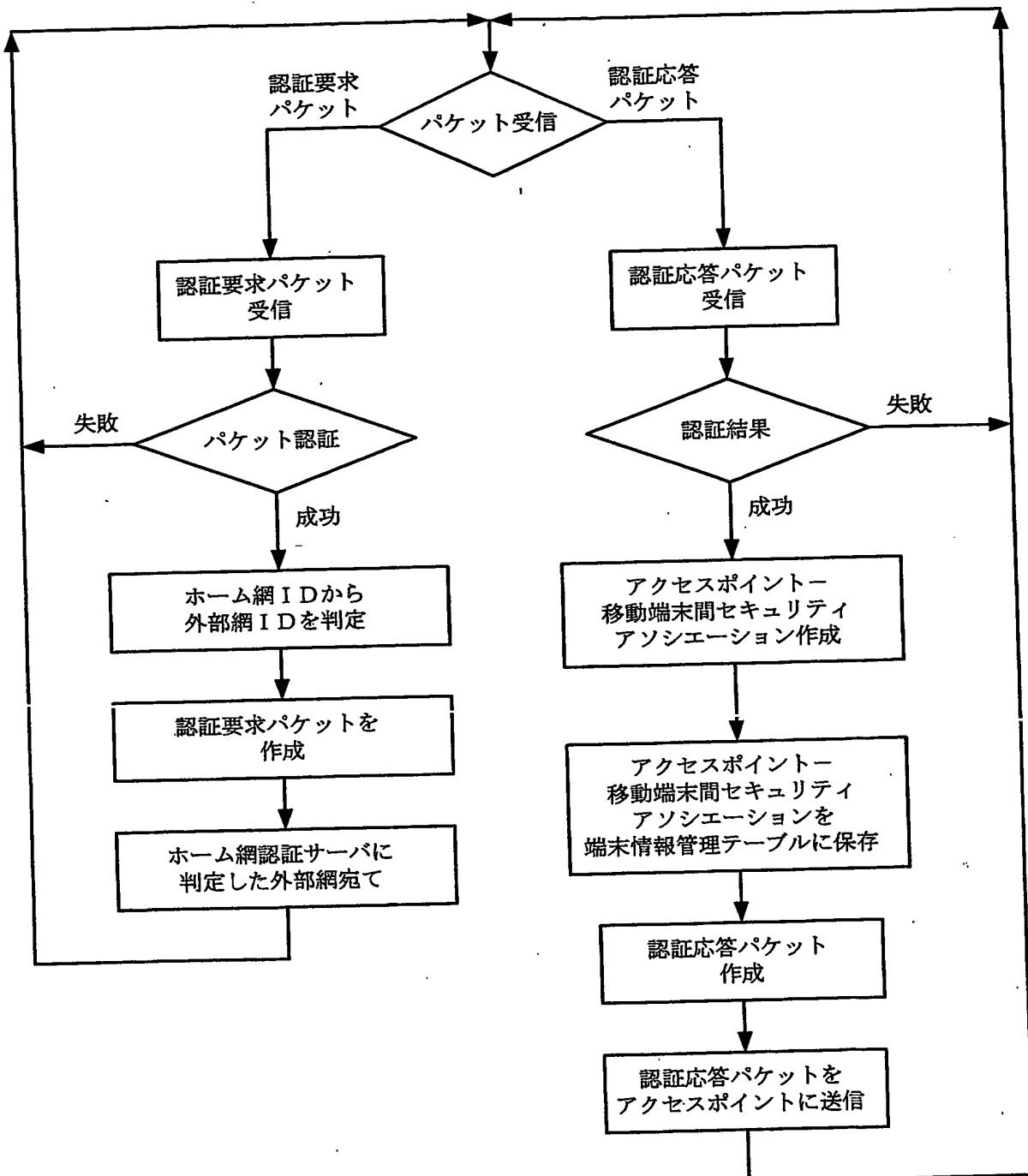
【図25】



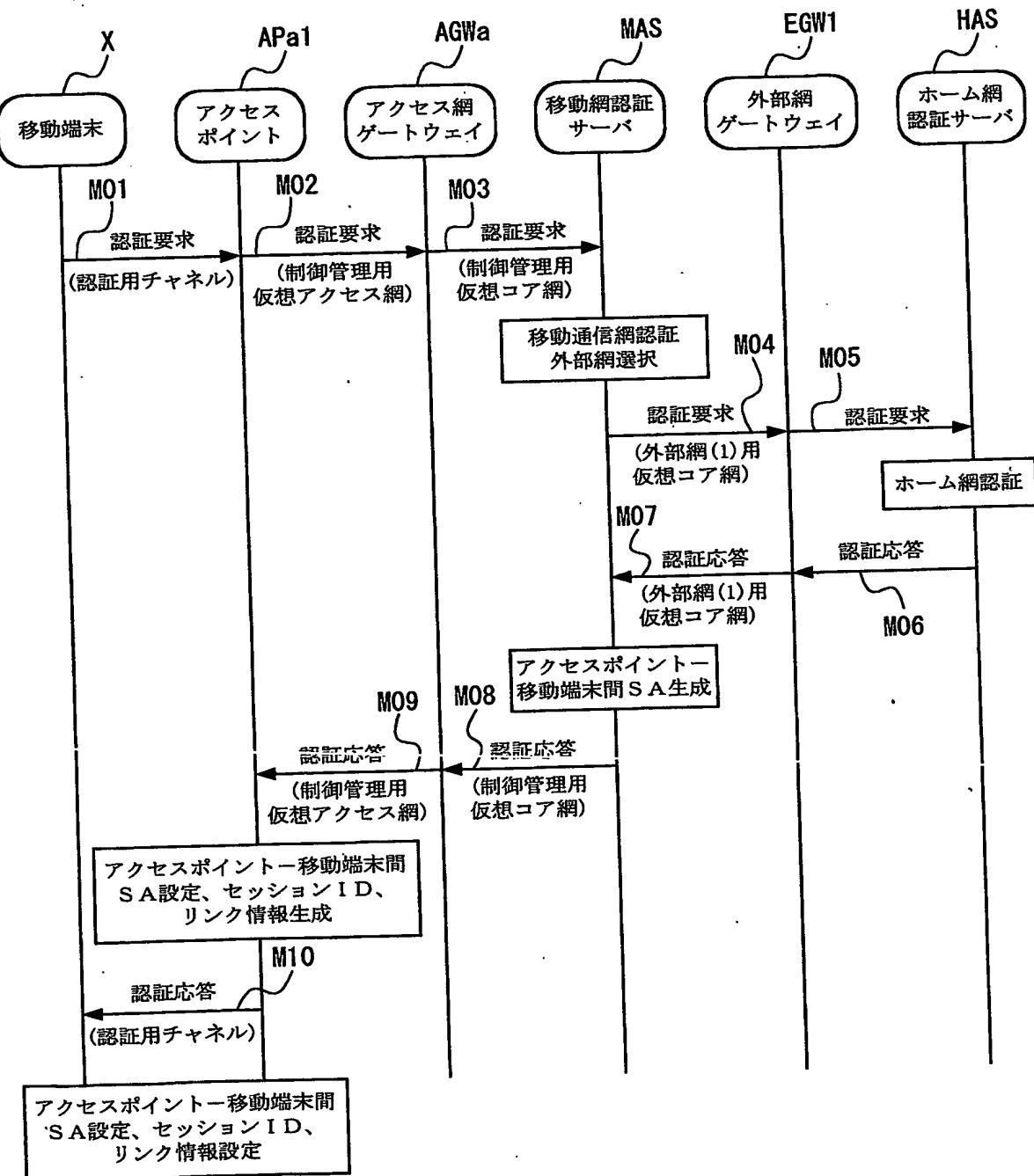
【図26】



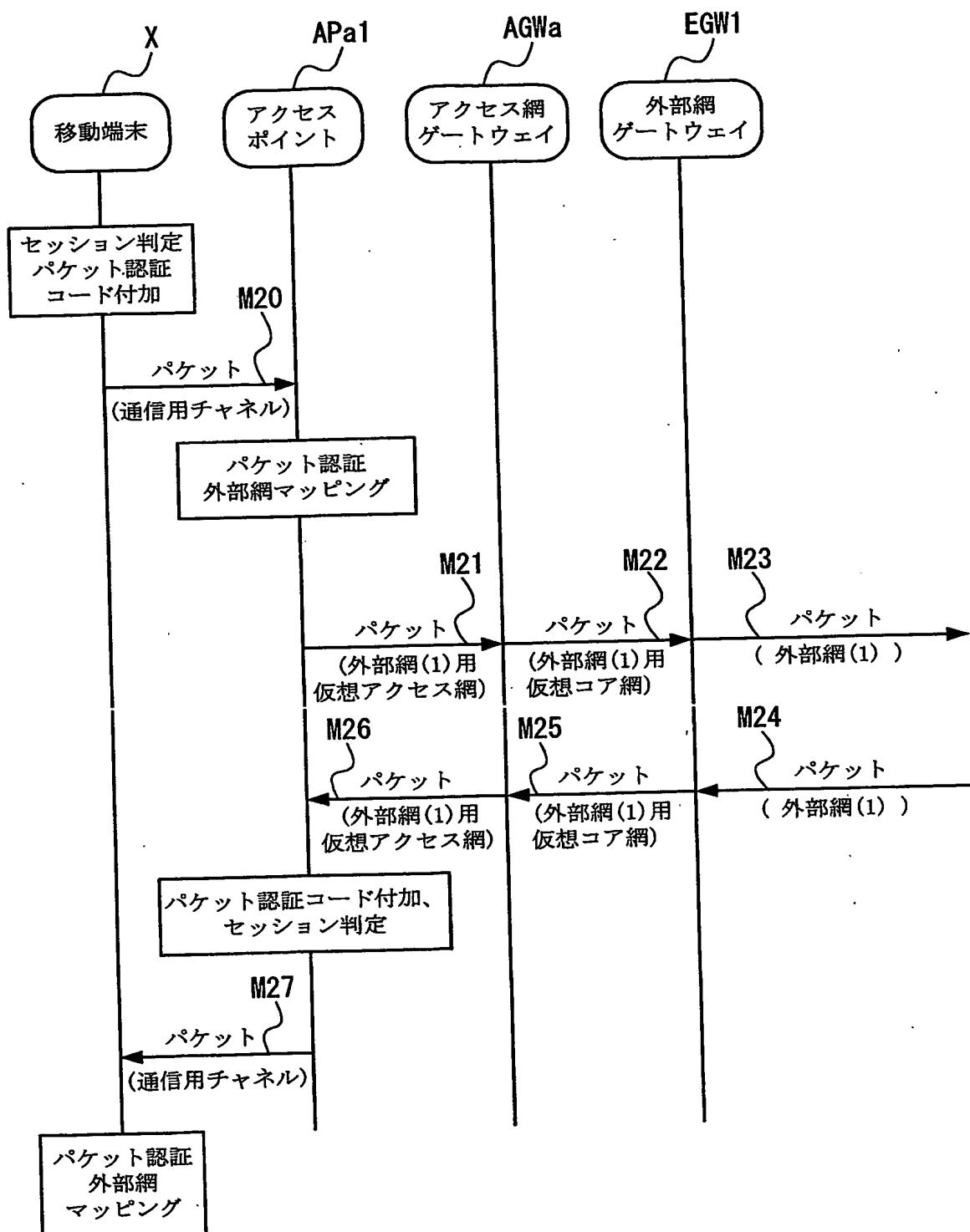
【図27】



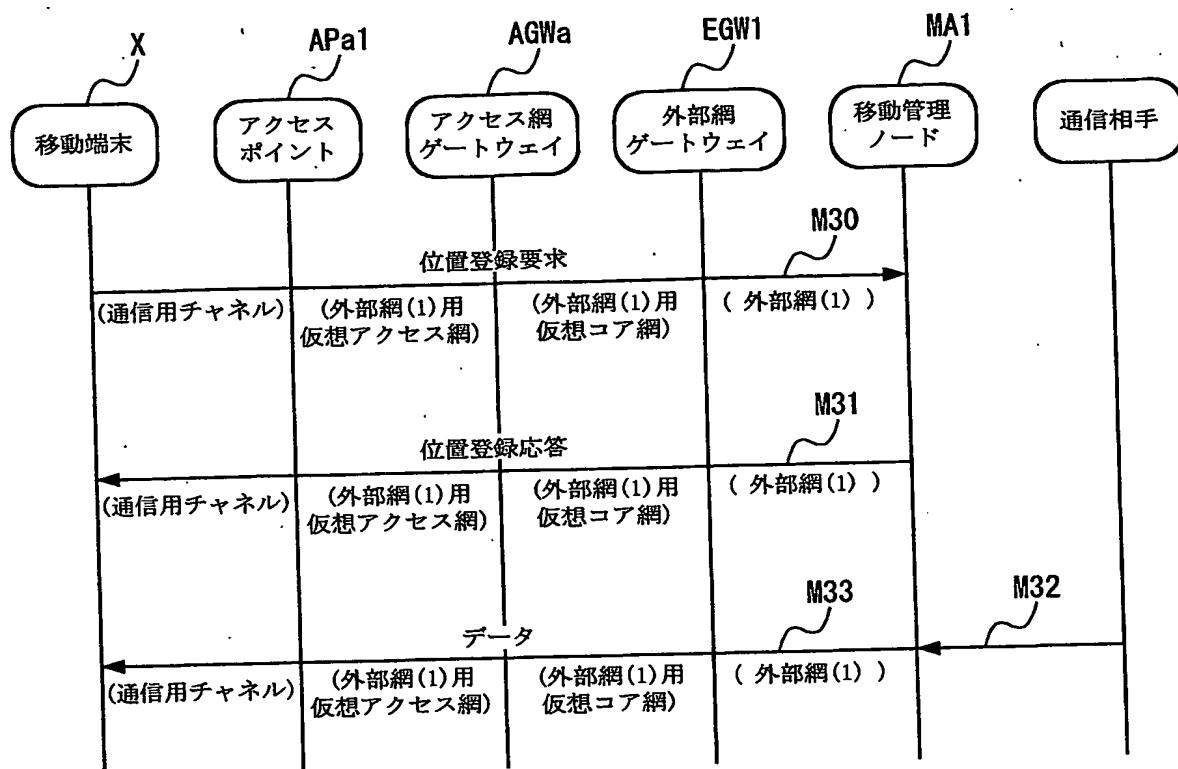
【図28】



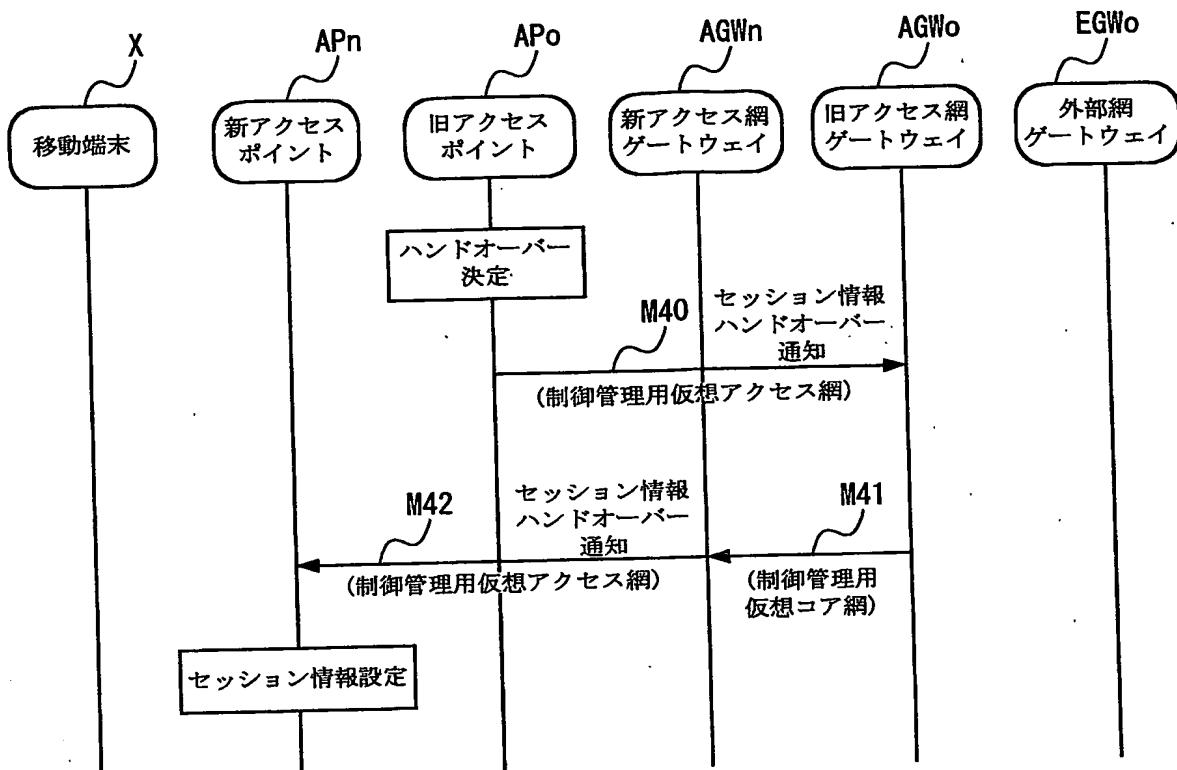
【図29】



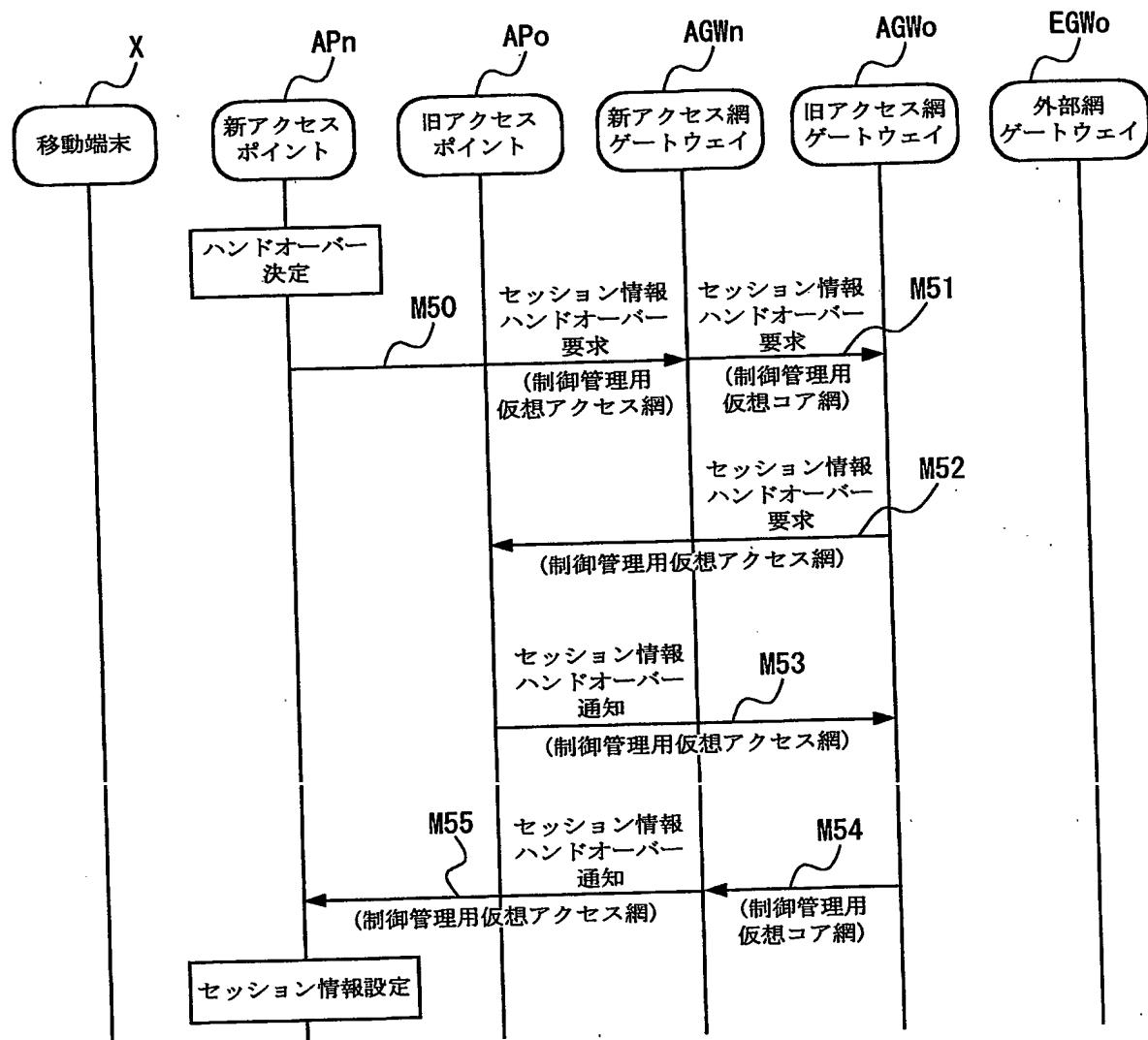
【図30】



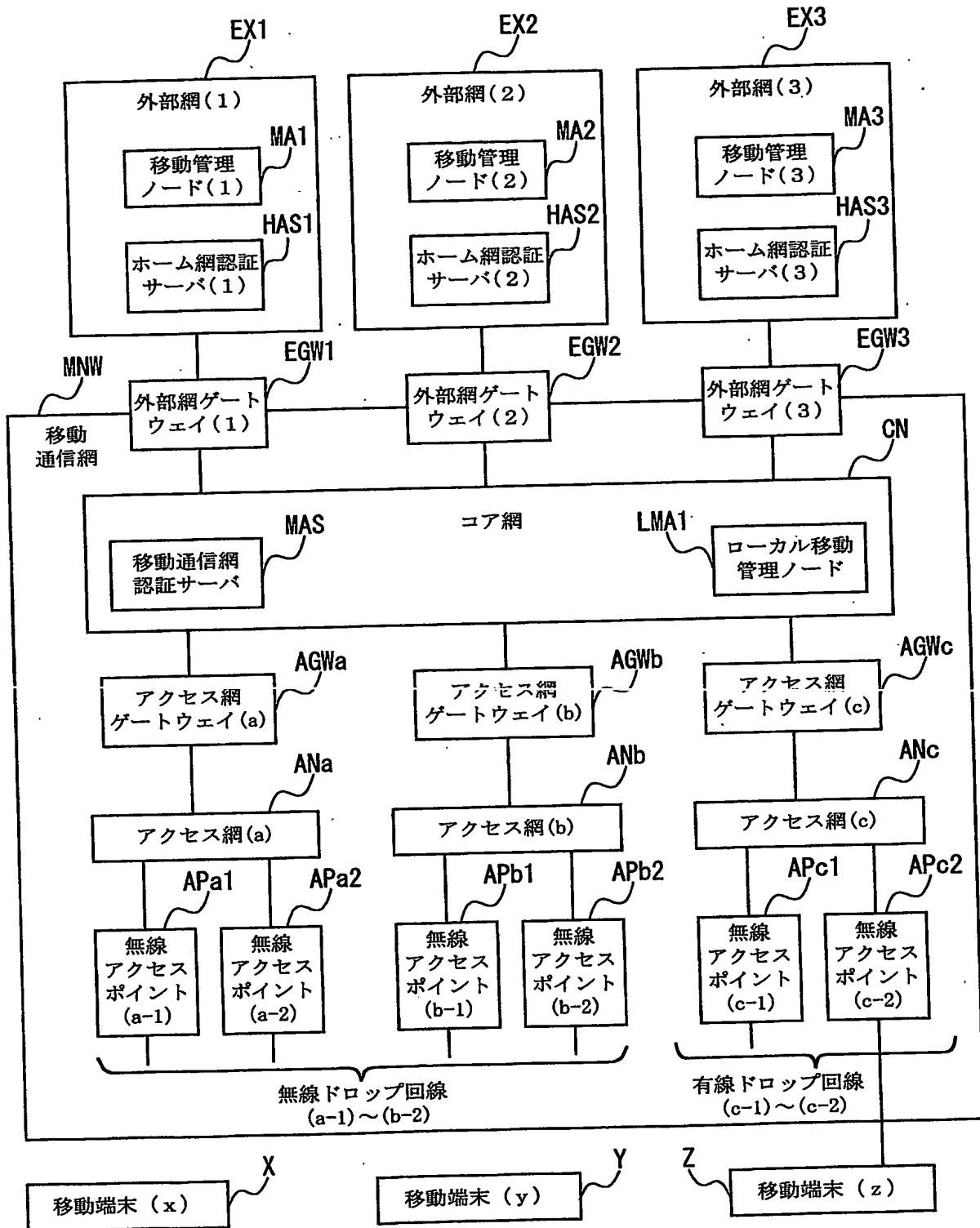
【図31】



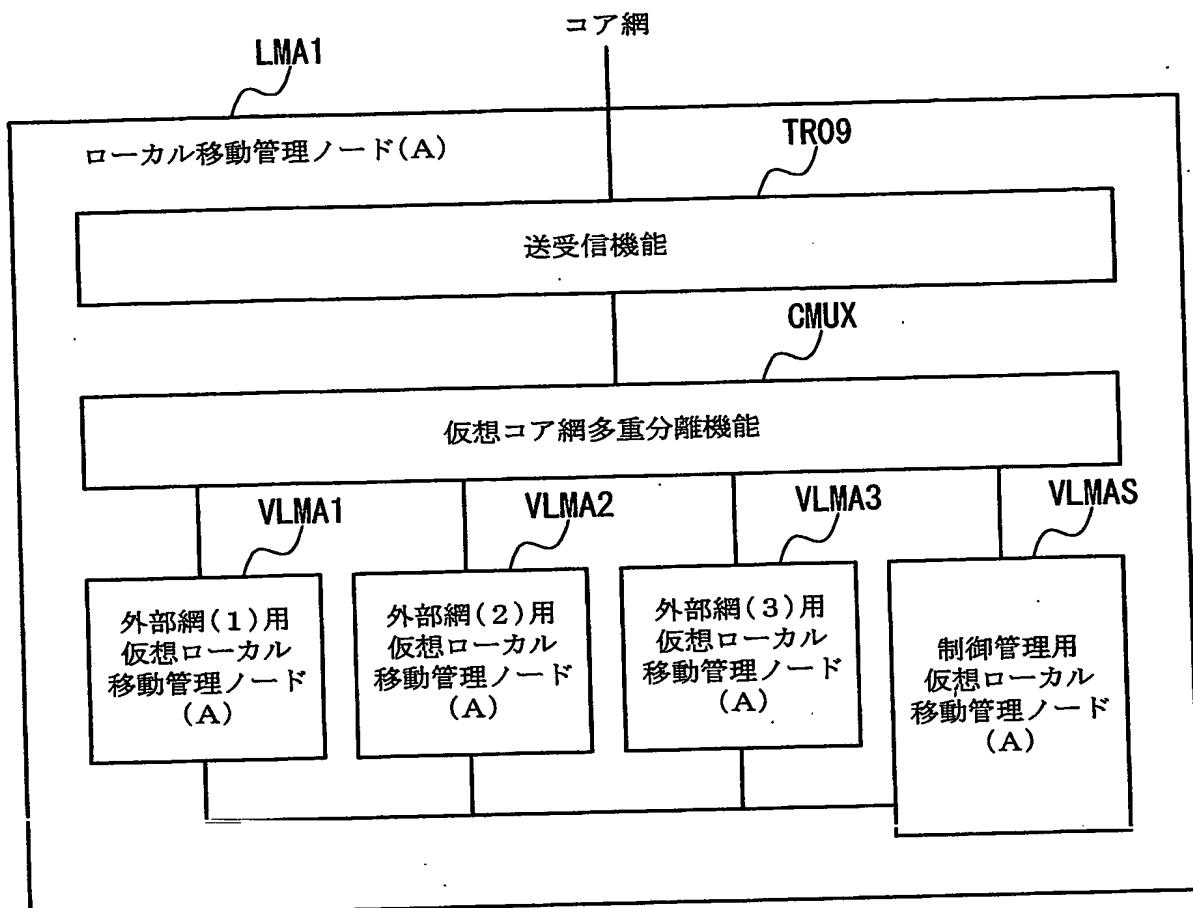
【図32】



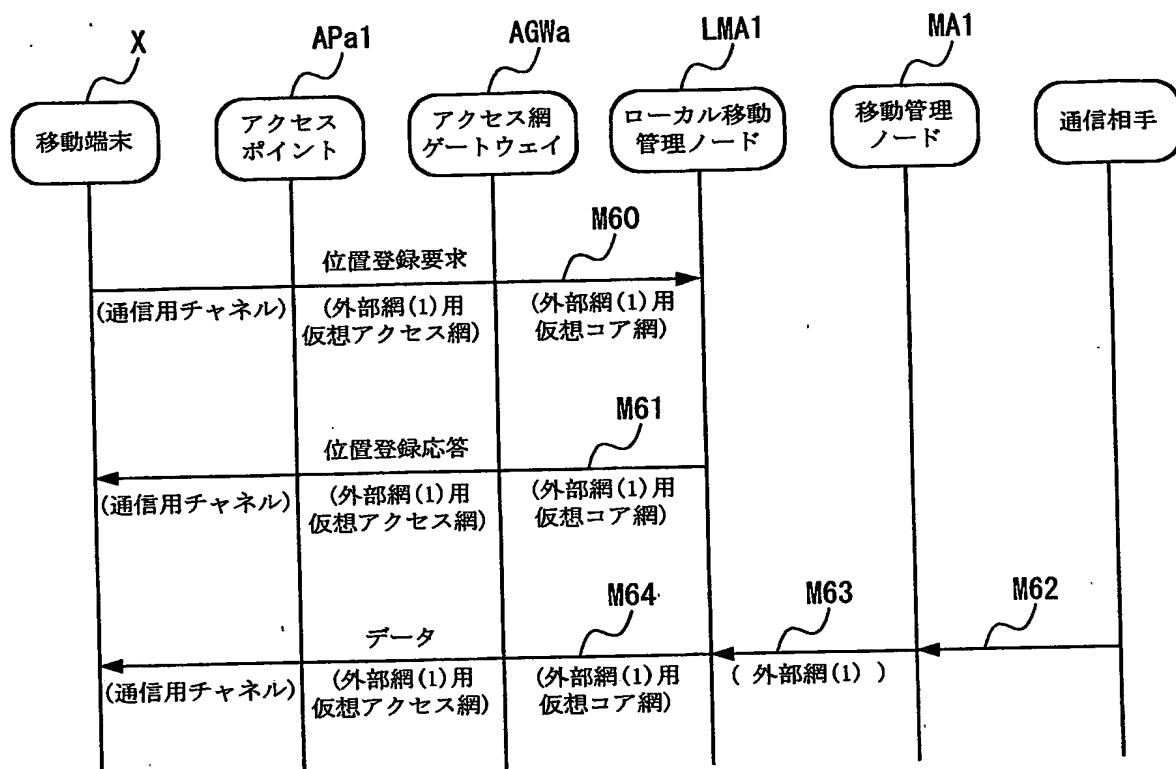
【図33】



【図34】



【図35】



【書類名】 要約書

【要約】

【課題】 移動端末で通信を行う場合の回線使用効率の改善を実現する移動通信網構成方式を提供する。

【解決手段】 移動端末は移動通信網のアクセスポイントとの間に接続したい網とのセッションを設定する手段を備える。移動通信網は仮想ネットワーク技術を利用して各種の網を多重する手段を備える。アクセスポイントは移動端末が設定したセッションを対応する仮想ネットワークに接続する手段を備え、さらに、移動端末が新しいアクセスポイント配下に移動した場合は、移動端末が前にいたアクセスポイントから新しいアクセスポイントへ、移動端末が設定したセッションの情報を転送する手段を備える。

【選択図】 図1

特2002-123502

認定・付加情報

特許出願の番号	特願2002-123502
受付番号	50200606151
書類名	特許願
担当官	第七担当上席 0096
作成日	平成14年 4月26日

<認定情報・付加情報>

【提出日】 平成14年 4月25日

次頁無

出願人履歴情報

識別番号 [00004237]

1. 変更年月日 1990年 8月29日

[変更理由] 新規登録

住 所 東京都港区芝五丁目7番1号  
氏 名 日本電気株式会社